ABSTRACT

HERMAN, AARON PAUL. Positive Root Bounds and Root Separation Bounds. (Under the direction of Hoon Hong.)

In this thesis, we study two classes of bounds on the roots of a polynomial (or polynomial system). A positive root bound of a polynomial is an upper bound on the largest positive root. A root separation bound of a polynomial is a lower bound on the distance between the roots. Both classes of bounds are fundamental tools in computer algebra and computational real algebraic geometry, with numerous applications. In the first part of the thesis, we study the *quality* of positive root bounds. Higher quality means that the relative over-estimation (the ratio of the bound and the largest positive root) is smaller. We find that all known positive root bounds can be arbitrarily bad. We then show that a particular positive root bound is tight for certain important classes of polynomials. In the remainder of the thesis, we turn to root separation bounds. We observe that known root separation bounds are usually very pessimistic. To our surprise, we also find that known root separation bounds are not compatible with the geometry of the roots (unlike positive root bounds). This motivates us to derive new root separation bounds. In the second part of this thesis, we derive a new root separation for univariate polynomials by transforming a known bound into a new improved bound. In the third part of this thesis, we use a similar strategy to derive a new improved root separation bound for polynomial systems.

Positive Root Bounds and Root Separation Bounds

by
Aaron Paul Herman

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Applied Mathematics

Raleigh, North Carolina

2015

APPROVED BY:

Erich Kaltofen	Seth Sullivant
Agnes Szanto	Elias Tsigaridas

Hoon Hong
Chair of Advisory Committee

DEDICATION

To my family.

BIOGRAPHY

Aaron P. Herman and his identical twin Jonathan were born in Winston Salem, North Carolina. Shortly thereafter, their family moved across the country to Bozeman, Montana where they remained until their father finished his PhD in Physics. The family then swapped coasts again, settling in Radford, Virginia. Aaron went to the College of William and Mary and started out as a Physics major. Two years of studying Physics taught Aaron that laboratories were not for him, so he switched to Mathematics. After graduating he enrolled in the PhD program at North Carolina State University. His post graduation goal is to once again switch coasts, and find a job in the Seattle, Washington area.

ACKNOWLEDGEMENTS

Special thanks to

- My advisor, Hoon Hong, for teaching me how to think. And, even more impressively, how to slow down.
- Elias Tsigaridas, for helping me have an adventure.
- The members of my PhD committee, for their excellent input.
- Jeff and the rest of the crew, for keeping things fun (and sane).
- Last but certainly not least, my family, for never ending support.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

In this thesis, we study two classes of bounds on the roots of a polynomial (or polynomial system). A positive root bound of a polynomial is an upper bound on the largest positive root. A root separation bound of a polynomial is a lower bound on the distance between the roots. Both classes of bounds are fundamental tools in computer algebra and computational real algebraic geometry, with numerous applications.

We first study positive root bounds. Consider the following example.

Example 1.1. Let $f = 2x^4 + 8x^3 + 8x^2 - 7x - 6$. The roots of f are plotted in Figure 1.1. The largest positive root of f is .86. Hence, any number greater than or equal to .86 is a positive root bound.

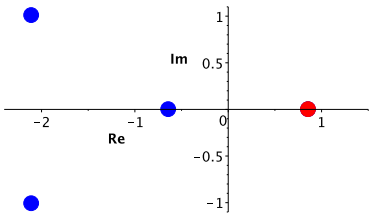

Figure 1.1: Roots of $f(x)$. The largest positive root is highlighted.

Note that the numbers greater than or equal to .86 are not all of equal *quality*. In this example, 8.6×10^{26} is a positive root bound, but it over-estimates the largest positive root by a factor of 10^{27}. A much better positive root bound can be found: .86, which is exactly the largest positive root. Unfortunately this is not a practical bound. If we were willing to do the work to compute all of the roots of f, we would have no need for a positive root bound in the

first place.

We now consider a well known due to Hong (B_H). The value of this positive root bound is $B_H(f) = 1.63$. This bound over-estimates the largest positive root by a factor of 1.9. Clearly, 1.63 is a positive root bound of higher quality than 1×10^{26}. This bound also has an advantage over the exact bound. Unlike the exact bound, the Hong bound can be computed *efficiently*. So we have a positive root bound that can be computed efficiently and is of very high quality for this polynomial. Could we have known before computing the bound that it would be high quality (or at the very least least, not arbitrarily bad)? We will answer this question in Chapter 3. □

Our main concern in Chapter 3 will be the quality of efficiently computable positive root bounds. Higher quality means that the relative over-estimation (the ratio of the bound and the largest positive root) is smaller. We report four findings.

1. Most known positive root bounds can be *arbitrarily bad*; that is, the relative over-estimation can approach infinity, even when the degree and the coefficient size are fixed.

2. When the number of sign variations is the same as the number of positive roots, the relative over-estimation of a positive root bound due to Hong (B_H) is at most *linear* in the degree, no matter what the coefficient size is.

3. When the number of sign variations is one, the relative over-estimation of B_H is at most *constant*, in particular 4, no matter what the degree and the coefficient size are.

In the remainder of the thesis, we study root separation bounds. Consider the following example.

Example 1.2. Let $f(x) = x^4 - 60x^3 + 1000x^2 - 8000x$. The roots of $f(x)$ are plotted in Figure 1.2. The lengths of the red line segments are the distances between the roots of $f(x)$. The root separation is the smallest of these distances. The root separation of $f(x)$ is $\sqrt{200}$ (≈ 14.14), so any number $\leq \sqrt{200}$ is a root separation bound.

As with positive root bounds, not all root separation bounds are of equal quality. For example, 1.00×10^{-100} is not a very good root separation bound. And also as with positive root bounds, there exist a root separation bound of perfect quality: $\sqrt{200}$. But computing the exact root separation is not practical, since the computation of the exact root separation requires the computation of all of the roots of f.

We now consider the well known Mahler-Mignotte bound (B_{MM}). The Mahler-Mignotte bound can be computed efficiently, and has a similar form to all other known efficiently computable root separation bounds. We have

$$B_{MM}(\, f(x)\,) \;=\; 8.26 \times 10^{-6}$$

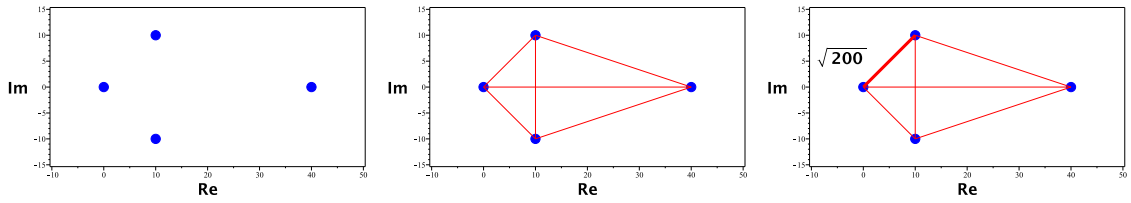

Figure 1.2: Roots of $f(x)$ (left), distances between roots (center), minimum separation highlighted (right)

Note that this value is much smaller than the exact root separation bound.

Now consider the polynomial $f(\,x/2\,)$. Clearly, the roots of $f(\,x/2\,)$ are the doubled roots of f. Hence the root separation of $f(\,x/2\,)$ is doubled. Naturally, we expect a root separation bound of $f(\,x/2\,)$ to be doubled as well. Let us see what happens:

$$B_{MM}(\,f(x/2)\,) \;=\; 1.05 \times 10^{-6}$$

It is not doubled; in fact, it is smaller! If we triple the roots, it turns out the Mahler-Mignotte bound is *even smaller*. It appears that the Mahler-Mignotte bound is not compatible with the geometry of the roots of f. □

It is well known that current root separation bounds are very pessimistic. It is less well known that root separation bounds do not scale correctly (as we see in the above example). So we have a challenge. Namely, we want to find new root separation bounds such that

1. the new bounds are less pessimistic (or almost always less pessimistic) than known bounds
2. the new bounds scale correctly
3. and of course, the new bounds can be computed efficiently.

The main contributions of Chapters 4 and Chapter 5 are two new root separation bounds which meet the challenge. The new bounds are derived by transforming a known root separation bound into a new improved root separation bound which meets the challenge. In Chapter 4, we transform the well known Mahler-Mignotte bound into a new improved bound. In Chapter 5, we transform a multivariate bound due to Emiris, Mourrain, and Tsigaridas [18]. Experimental evidence indicates that the improvement is usually very large, especially when the magnitude of the roots are different from 1.

Chapter 2

Background

This thesis considers three topics: Positive Root Bounds (Chapter 3), Root Separation Bounds of Univariate Polynomials (Chapter 4), and Root Separation Bounds of Polynomial Systems (Chapter 5). In this chapter, we present background material for each topic. For all three topics, we define the category of bounds being considered. We then re-derive previously discovered results that are necessary in later chapters.

2.1 Positive Root Bounds of Univariate Polynomials

In this section, we discuss positive root bounds. A positive root bound of a polynomial is an upper bound on the largest positive root. Positive root bounds play an important role in computer algebra and computational real algebraic geometry (see [53, 50, 47] for some applications). As a consequence, there has been intensive effort on finding such bounds [30, 10, 2, 27, 49, 2, 3, 22, 6].

First, we formally define a positive root bound. Let $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{R}[x]$ with positive leading coefficient and at least one positive root.

Notation 2.1. $x^*(f) =$ the largest positive root of f.

Definition 2.1. $B \in \mathbb{R}^+$ is a *positive root bound* if $B \geq x^*(f)$.

Example 2.1. Consider again the example from the introduction. Let $f = 2x^4 + 8x^3 + 8x^2 - 7x - 6$. The roots of f are plotted in Figure 2.1. The largest positive root of f is $x^*(f) = .86$. Hence, any number greater than or equal to .86 is a positive root bound. □

Some well known positive root bounds are listed below.

- Lagrange, 1798 [30]

$$B_L(f) = 1 + \left(\max_{\substack{q \\ a_q < 0}} \left| \frac{a_q}{a_d} \right| \right)^{\frac{1}{d-m}}$$

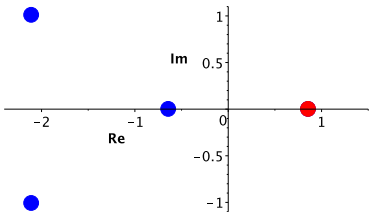

Figure 2.1: Roots of $f(x)$. The largest positive root is highlighted.

where $m = \max\{q : a_q < 0\}$.

- Cauchy, 1829 [10]

$$B_C(f) = \max_{\substack{q \\ a_q<0}} \left| \frac{\lambda a_q}{a_d} \right|^{\frac{1}{d-q}}$$

where $\lambda = \#\{q : a_q < 0\}$.

- Kioustelidis, 1986 [27]

$$B_K(f) = 2 \max_{\substack{q \\ a_q<0}} \left| \frac{a_q}{a_d} \right|^{\frac{1}{d-q}}$$

- Hong, 1998 [22]

$$B_H(f) = 2 \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0 \\ p>q}} \left| \frac{a_q}{a_p} \right|^{\frac{1}{p-q}}$$

Stefanescu, Akritas, Strzebonksi, Vigklas, Batra and Sharma [49, 2, 6] extended the above bounds by splitting single monomials as sums of several monomials and considering different groupings of positive and negative monomials. Batra and Sharma [6] showed that the tightest bound in their framework improves on B_H by at most a constant. It is not clear whether a similar statement holds for the framework in [2], but we have not been able to find a counter example. Complex root bounds (upper bounds on the magnitude of the roots) are by definition positive root bound as well (see [28, 20, 29, 35, 25, 23, 24, 41, 4, 26, 16]).

Of the positive root bounds listed above, the Hong bound will feature most prominently in this thesis. To the best of the author's knowledge, the Hong bound is the tightest *linear complexity* positive root bound. It is not obvious that the Hong bound can be computed in linear time, since it involves a max over a min. However, Melhorn and Ray [36] found an ingenious way to compute it in linear time. Their algorithm will be crucial to the complexity results in Chapter 4.

In the remainder of this section, we will consider the Hong bound. First, we re-derive the

Hong bound using a similar argument to that of Hong in [22]. Then we discuss the algorithm of Melhorn and Ray.

2.1.1 Derivation of the Hong Bound

In this subsection, we re-derive the Hong bound. To the best of the author's knowledge, every positive root bound is derived using the following strategy:

1. Partition the monomials of f into a sum of the form

$$f = f_1 + \cdots + f_r$$

   where every part has the form

$$f_i(x) = a_p x^p + \sum_{q \in Q} a_q x^q$$

   with $a_q < 0$ and $q < p$ for all $q \in Q$.

2. Find a positive root bound for each partition.

3. Define $B(f)$ as the maximum of the positive root bounds derived in Step 2.

We will use this strategy to re-derive the bound of Hong. We will utilize the following Lemma, which was first presented by Kioustelidis in [27].

Lemma 2.1 (Kioustelidis, 1986 [27])**.** Suppose f has the form

$$f = a_p x^p + \sum_{q \in Q} a_q x^q$$

with $a_p > 0$, $a_q < 0$ and $q < p$ for all $q \in Q$. Then

$$f(x) \geq 0 \quad \text{for all} \quad x \geq B$$

where

$$B = 2 \max_{q \in Q} \left| \frac{a_q}{a_d} \right|^{\frac{1}{d-q}}$$

Proof. Let $x \geq B$. We have

$$f(x) = a_p x^p + \sum_{q \in Q} a_q x^q$$

$$
\begin{aligned}
&= a_p x^p \left(1 + \sum_{q \in Q} \frac{a_q}{a_p} x^{q-p} \right) \\
&= a_p x^p \left(1 - \sum_{q \in Q} \left| \frac{a_q}{a_p} \right| x^{q-p} \right) \\
&= a_p x^p \left(1 - \sum_{q \in Q} \frac{\left| \frac{a_q}{a_p} \right|}{x^{d-p}} \right) \\
&\geq a_p x^p \left(1 - \sum_{q \in Q} \frac{\left| \frac{a_q}{a_p} \right|}{B^{p-q}} \right) && \text{since } x \geq B \qquad (2.1)
\end{aligned}
$$

To complete the proof, we will show that right term in the right hand side of (2.1) is positive. We have

$$
\begin{aligned}
1 - \sum_{q \in Q} \frac{\left| \frac{a_q}{a_p} \right|}{B^{p-q}} &= 1 - \sum_{q \in Q} \frac{\left| \frac{a_q}{a_p} \right|}{\left(2 \max_{q \in Q} \left| \frac{a_q}{a_p} \right|^{\frac{1}{p-q}} \right)^{p-q}} \\
&= 1 - \sum_{q \in Q} \frac{\left| \frac{a_q}{a_p} \right|}{2^{p-q} \max_{q \in Q} \left| \frac{a_q}{a_p} \right|} \\
&\geq 1 - \sum_{q \in Q} \frac{\max_{q \in Q} \left| \frac{a_q}{a_p} \right|}{2^{p-q} \max_{q \in Q} \left| \frac{a_q}{a_p} \right|} \\
&= 1 - \sum_{q \in Q} \left(\frac{1}{2} \right)^{p-q} \\
&\geq 1 - \sum_{q < p} \left(\frac{1}{2} \right)^{p-q} \\
&\geq 2 - \sum_{q \leq p} \left(\frac{1}{2} \right)^{p-q} && \text{since the summand is 1 when } q = p \\
&> 2 - \sum_{i=0}^{\infty} \left(\frac{1}{2} \right)^{i} \\
&= 0 && (2.2)
\end{aligned}
$$

Combining (2.1) and (2.2) we have

$$f(x) \geq 0$$

We have completed the proof of the Lemma. □

To derive the Hong bound, we will partition f into a sum of polynomials of the form of the polynomial in Lemma 2.1. There will be one part for every positive term of f. Negative monomials will matched with the positive monomial that minimizes

$$\left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}}, \quad p > q$$

This choice of partition is motivated by the simple observation that a *smaller* positive root bound is a *tighter* positive root bound.

Theorem 2.1 (Hong, 1998 [22] [1])**.**

$$x^*(f) \leq B_H(f)$$

Proof. Let

$$\mu(q) = \arg\min_{p>q} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}}$$

Consider the following partition of f:

$$f = \sum_{\substack{p \\ a_p>0}} f_p \qquad \text{where} \qquad f_p = a_p x^p + \sum_{\substack{q \\ a_q<0 \\ \mu(q)=p}} a_q x^q \tag{2.3}$$

Note that every f_p has the form of the polynomial in Lemma 2.1. Hence

$$f_p(x) \geq 0 \text{ for all } x \geq B_p \tag{2.4}$$

where

$$B_p = 2 \max_{\substack{q \\ a_q<0 \\ \mu(q)=p}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}} = 2 \max_{\substack{q \\ a_q<0 \\ \mu(q)=p}} \left|\frac{a_q}{a_{\mu(q)}}\right|^{\frac{1}{\mu(q)-q}}$$

Combining (2.3) and (2.4) we have

$$f(x) \geq 0 \quad \text{for all} \quad x \geq \max_{\substack{p \\ a_p>0}} B_p \tag{2.5}$$

[1] In [22], $B_H(f)$ is derived in a more general setting: absolute positivity of multivariate polynomials. Here we simplify the proof by showing only that $B_H(f)$ is a positive root bound.

To complete the proof, we will simplify the right inequality of (2.5). We have

$$\begin{aligned}
\max_{\substack{p \\ a_p>0}} B_p &= 2 \max_{\substack{p \\ a_p>0}} \max_{\substack{q \\ a_q<0 \\ \mu(q)=p}} \left|\frac{a_q}{a_{\mu(q)}}\right|^{\frac{1}{\mu(q)-q}} \\
&= 2 \max_{\substack{q \\ a_q<0}} \left|\frac{a_q}{a_{\mu(q)}}\right|^{\frac{1}{\mu(q)-q}} \\
&= 2 \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0 \\ p>q}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}} && \text{since } \mu(q) = \arg\min_{p>q} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}} \\
&= B_H(f) && (2.6)
\end{aligned}$$

Combining (2.5), (2.6), and the fact that f has positive leading coefficient, we have

$$x^*(f) \leq B_H(f)$$

□

2.1.2 Computing the Hong Bound in Linear Time

In this subsection, we discuss Melhorn and Ray's algorithm [36] for computing B_H. To derive the algorithm, they interpret B_H geometrically. Then, using a strategy inspired by the Fast Convex Hull algorithm, they compute B_H in $\mathcal{O}(d)$ algebraic operations and comparisons.

Consider the following rewrite:

$$B_H(f) = 2\,\mathcal{H}(f), \quad \text{where} \quad \mathcal{H}(f) = \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0 \\ p>q}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}}$$

We will compute

$$\log\left(\mathcal{H}(f)\right) \;=\; \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0 \\ p>q}} \frac{\log(|a_q|) - \log(|a_p|)}{p-q} \;=\; \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0 \\ p>q}} \frac{b_p - b_q}{p-q}$$

where $b_i = -\log(|a_i|)$. The current problem is interpreted as a geometric problem by viewing $(b_p - b_q)/(p-q)$ as the slope of the line between the points $v_p = (p, b_p)$ and $v_q = (q, b_q)$. We distinguish between two classes of points. A point is a *positive point* point if $a_i > 0$. A point is

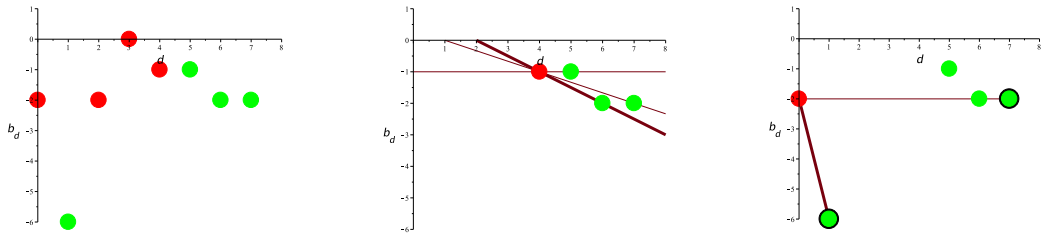

Figure 2.2: All positive and negative points (left), computation of s_4 (middle), computation of s_0 (right)

a *negative point* if $a_i < 0$. Under this interpretation, we observe that the quantity

$$s_q = \min_{\substack{p \\ a_p>0 \\ p>q}} \frac{b_p - b_q}{p - q}$$

is the slope of the tangent line of v_q and the set of positive points $\mathcal{P}_q = \{v_p : a_p > 0, p > q\}$. Equivalently, s_q is the slope of the tangent line of v_q and the *Lower Hull* of $\mathcal{P}_q$. We want to find the maximum value of s_q over all of the negative points.

Example 2.2. We illustrate the concepts above with a simple example. Let $f = 4x^7 + 4x^6 + 2x^5 - 2x^4 - x^3 - 4x^2 + 64x - 4$. The positive points are

$$(7, -\log(4)),\ (6, -\log(4)),\ (5, -\log(2)),\ (1, -\log(64)) = (7, -2),\ (6, -2),\ (5, -1),\ (1, -6)$$

and the negative points are

$$(4, -\log(2)),\ (3, -\log(1)),\ (2, -\log(4)),\ (0, -\log(4)) = (4, -1),\ (3, 0),\ (2, -2),\ (0, -2).$$

In the left hand plot of Figure 2.2, the positive points are plotted in green and the negative points are plotted in red.

Consider the negative point $v_4 = (4, -1)$. The value of s_4 is the minimum of the slopes of the lines in the middle plot of Figure 2.2. The line which achieves the minimum slope is highlighted.

Consider the negative point $v_1 = (0, -2)$. The value of s_0 is the minimum of the slopes of every line between v_1 and a positive point. Clearly this minimum is attained by a line between v_1 and a point in the lower hull of the positive points. Hence we need only to calculate the minimum of the slopes of lines connecting v_0 and points on the lower hull. In the right hand plot of Figure 2.2, the positive points in the lower hull are circled. The value of s_0 is the

minimum of the slopes of the two lines. □

To compute the quantity $\log(\mathcal{H}(f))$ in $\mathcal{O}(d)$ algebraic operations and comparisons, we use an algorithm inspired by the Fast Convex Hull algorithm of computational geometry. At each step of the algorithm, we store and potentially update the following:

$$\begin{aligned} s_{q^*} &= \text{the maximum value of } s_q \text{ over the set of negative points} \\ \mathcal{L} &= \text{the lower hull of the set of positive points} \end{aligned}$$

We process the points v_i from right to left (equivalently: from the points of the highest degree coefficients to lower degree coefficients).

- If v_i is a positive point, we update $\mathcal{L}$ using the standard update from the Fast Convex Hull algorithm.
- If v_i is a negative point, we update s_{q^*} (if necessary).

The total work done processing the positive points is $\mathcal{O}(d)$, since the Fast Convex Hull algorithm is $\mathcal{O}(d)$[2]. It is not obvious that we can process the negative points in a total of $\mathcal{O}(d)$ algebraic operations and comparisons. In a naive algorithm, we would calculate s_i for every negative point. Furthermore, in a naive calculation of s_i we would iterate through $\mathcal{L}$ starting from the leftmost (or rightmost) point until we find the point of tangency, then use the point of tangency to calculate s_i. This naive strategy would require $\mathcal{O}(d)$ operations for every negative point.

To speed up the processing of the negative coefficients, we make the following observations.

Observation 2.1. Let v_{q_1} and v_{q_2} be two negative points with $q_1 < q_2$. Note that by definition v_{q_1} lies to the left of v_{q_2} and $\mathcal{P}_{q_1} \supseteq \mathcal{P}_{q_2}$. Let

$$\begin{aligned} \mathcal{L}_{q_2} &= \text{the Lower Hull of } \mathcal{P}_{q_2} \\ \mathcal{L}_{q_1} &= \text{the Lower Hull of } \mathcal{P}_{q_1} \\ \mathcal{T} &= \text{the tangent point of } v_{q_2} \text{ and } \mathcal{L}_{q_2} \\ l &= \text{the line from } v_{q_2} \text{ to } \mathcal{T} \end{aligned}$$

Then

1. If $\mathcal{T} \in \mathcal{L}_{q_1}$ and v_{q_1} lies above l, then $s_{q_1} \leq s_{q_2}$.
2. If $\mathcal{T} \in \mathcal{L}_{q_1}$ and v_{q_1} lies below l, then the tangent point of v_{q_1} and $\mathcal{L}_{q_1}$ lies to the right of $\mathcal{T}$, and $s_{q_1} \geq s_{q_2}$.

[2]Under the assumption that the points are already sorted from left to right.

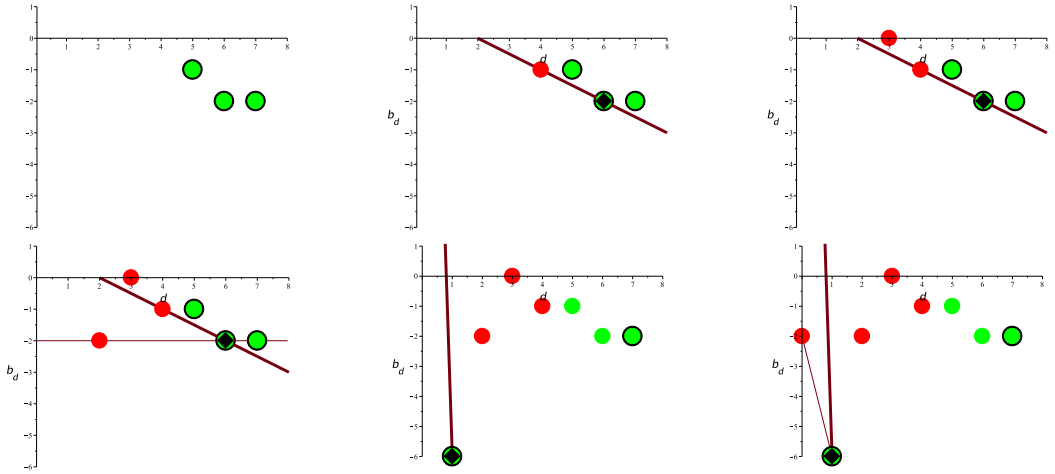

Figure 2.3: Computation of $\mathcal{H}(f)$

3. If $\mathcal{T} \notin \mathcal{L}_{q_1}$, then every point to the left of $\mathcal{T}$ in $\mathcal{L}_{q_2}$ is not in $\mathcal{L}_{q_1}$.

Example 2.3. We illustrate the above observations and the main ideas behind the algorithm *Compute*$\mathcal{H}$ with the same example as before. We will process the points from right to left and at the end of the computation we will have found $\mathcal{H}(f)$. We will use Observation 2.1 to avoid unnecessary computations.

v_7: Since v_7 is a positive point, we add the point to the (currently empty) lower hull $\mathcal{L}$.

v_6: Since v_6 is a positive point, we compute the lower hull of $\mathcal{L} \cup v_6$. Since the lower hull of two (non vertical) points is simply the same two points, we have $\mathcal{L} = (v_6, v_7)$.

v_5: Since v_5 is a positive point, we compute the lower hull of $\mathcal{L} \cup v_5$. We use the standard fast convex hull update. We first set

$$\mathcal{L} = (v_5, v_6, v_7)$$

then check if we need to delete points from $\mathcal{L}$. We consider the first three points of $\mathcal{L}$. Since a right turn is made on the path $v_7 \rightarrow v_6 \rightarrow v_5$, we do not have to delete any points from $\mathcal{L}$. See the top left of Figure 2.3.

v_4: Since v_4 is a negative point and we have yet to compute a value of s_{q^*}, we compute s_4. To do so we search through $\mathcal{L}$ from the left until we find the tangent line with smallest slope. We store the current maximum $s_{q^*} = s_4$, the line l whose slope is s_4 (the line from v_4 to v_6), and the tangent point $\mathcal{T} = v_6$. See the top middle of Figure 2.3.

v_3: Since v_3 is a negative point, we potentially have to update s_{q^*}. However, v_3 lies above the line l. Hence s_3 will clearly be smaller than s_4, and there is no need to compute s_3 (Observation 2.1.1). See the top right of Figure 2.3.

v_2: Since v_2 is a negative point, we potentially have to update s_{q^*}. We notice that v_2 lies below l. Hence we cannot use Observation 2.1.1 to avoid the computation of s_2. However, we can use Observation 2.1.2 to speed up the computation. We search through $\mathcal{L}$ to the right starting at $\mathcal{T} = v_6$ to find the value of s_3. In this manner, we avoid having to calculate the slope of the line connecting v_3 and v_5. We note that s_2 is larger than s_4, hence we set $s_{q^*} = s_2$. See the bottom left of Figure 2.3.

v_1: Since v_1 is a positive point, we update $\mathcal{L}$. We calculate the lower hull of

$$\mathcal{L} \cup v_1 = (v_5, v_6, v_7) \cup (v_1)$$

We first set

$$\mathcal{L} = (v_1, v_5, v_6, v_7)$$

Then consider the first three points in $\mathcal{L}$. Since a left turn is made on the path $v_6 \rightarrow v_5 \rightarrow v_1$, we delete v_5 from $\mathcal{L}$. We now have

$$\mathcal{L} = (v_1, v_6, v_7)$$

Again, we consider the first three points in $\mathcal{L}$. Since a left turn is made on the path $v_7 \rightarrow v_6 \rightarrow v_1$, we delete v_6 from $\mathcal{L}$. Note that $\mathcal{T} = v_6$ was deleted from $\mathcal{L}$, as was every point to the left of $\mathcal{T}$ in $\mathcal{L}$ (in this case, the only point to the left was v_5), confirming Observation 2.1.3.

Since the current tangent point (v_6) was deleted from $\mathcal{L}$, we will reset l and $\mathcal{T}$:

$$\begin{aligned} \mathcal{T} &= v_1 \\ l &= \text{the line from } v_1 \text{ to } (0, \infty) \end{aligned}$$

See the bottom middle of Figure 2.3.

v_0: Since v_0 is a negative point, we potentially update s_{q^*}. We notice that v_0 lies below l. Hence we cannot use Observation 2.1.1 to avoid the computation of s_0. We search for the point of tangency of v_0 and $\mathcal{L}$ starting from $\mathcal{T} = v_1$, and find that v_1 is the point of tangency. The slope of the line from v_0 to v_1 is s_0. We see that this number is smaller than $s_{q^*} = s_2$ (which is the slope of the line from v_3 to v_6). Hence we do not update s_{q^*}.

Finally, all of the points have been processed, and we return $s_{q^*} = \mathcal{H}(f)$. □

Let us summarize the strategy in the above example. We use Observation 2.1 to efficiently process the points from right to left. For a negative point v_i, we first check if v_i above l. If v_i lies above l, then there is no need to calculate s_i (Observation 2.1.1). If v_i lies below l, we will search through $\mathcal{L}$ to the right *starting at* $\mathcal{T}$ (Observation 2.1.2). We use the new point of tangency to calculate s_i. Once the point of tangency is found, we set $\mathcal{T}$ to be the new point of tangency and l to the line from v_i to $\mathcal{T}$. When processing a positive point, we potentially remove $\mathcal{T}$ from $\mathcal{L}$. If $\mathcal{T}$ is removed from $\mathcal{L}$ we set $\mathcal{T}$ to be the left-most point in $\mathcal{L}$. When later negative points are processed, no iteration to the right in $\mathcal{L}$ will traverse an edge that has already been traversed (Observation 2.1.3). When $\mathcal{T}$ is reset, we set l to be the line from $\mathcal{T}$ to $(0, \infty)$, so that the next negative point is guaranteed to be below l.

We are now ready to present the algorithm $Compute\mathcal{H}$ (Algorithm 3) and discuss its complexity (Theorem 2.2). We make the crucial observation that no logarithms are necessary for the computation of $\mathcal{H}(f)$. By taking advantage of the simple fact that

$$\log(A) \leq \log(B) \leq A \leq B$$

we can modify the algorithm discussed above to avoid logarithm computations.

For the following algorithms:

- We represent points $(i, -\log(|a_i|)$ with the pair $(i, |a_i|)$.
- For $\mathcal{P}_1$ and $\mathcal{P}_2$ represented by $(p_1, |a_{p_1}|)$ and $(p_2, |a_{p_2}|)$ respectively, let

$$\mathcal{S}_{\mathcal{P}_1,\mathcal{P}_2} = \left(\frac{|a_{p_2}|}{|a_{p_1}|}\right)^{\frac{1}{p_1 - p_2}}$$

- For $\mathcal{P}_1$ and $\mathcal{P}_2$ represented by $(p_1, |a_{p_1}|)$ and $(p_2, |a_{p_2}|)$ respectively, the line from $\mathcal{P}_1$ to $\mathcal{P}_2$ is represented by

$$(\,(p_1, |a_{p_1}|),\, (p_2, |a_{p_2}|)\,)$$

Algorithm 1: *LowerHullUpdate*

Input : $\mathcal{L}$ = a list of points which form a lower hull, sorted from left to right.
$\mathcal{P}$ = a point to the left of L. $\mathcal{T}$ = a point in L. l = a line.
Output: $(\mathcal{L}', \mathcal{T}', l')$ where $\mathcal{L}'$ = the lower hull of $\mathcal{P} \cup \mathcal{L}$. $\mathcal{T}' = \mathcal{T}$ if $\mathcal{T} \in \mathcal{L}'$. Otherwise $\mathcal{T} = \mathcal{P}$. $l' = l$ if $\mathcal{T} \in \mathcal{L}'$. Otherwise l =the line from $\mathcal{P}$ to $(0, \infty)$.

```
1  begin
2      L' ← (P, L);
3      T' ← T;
4      l' ← l;
5      P1, P2, P3 ← the first 3 elements of L';
6      while size(L') > 2 and S_{P1,P2} > S_{P2,P3} // A right hand turn is made on the
           path P1 → P2 → P3
7      do
8          Remove P2 from L';
9          if P2 = T then
10             T' ← P;
11             l' ←the line from P to (0, ∞);
12         P1, P2, P3 ← the first 3 elements of L;
13 end
```

Algorithm 2: *TangentPoint*

Input : $\mathcal{L}$ = a list of points which form a lower hull, sorted from left to right.
$\mathcal{P}$ = a point to the left of $\mathcal{L}$.
$\mathcal{T}$ = a point in $\mathcal{L}$.
Output: $\mathcal{T}'$: The tangent point of $\mathcal{P}$ and the points to the right of $\mathcal{T}$ in $\mathcal{L}$.

```
1  begin
2      T' ← T;
3      if T' is not the right most point in L then
4          Y ← the point to the right of T' in L;
5          while T' is not the rightmost point in L and S_{P,T'} > S_{P,Y} // The slope of the
               line from P to T' is greater than the slope of the line from P
               to Y
6          do
7              T' ← Y;
8  end
```

Algorithm 3: *Compute*$\mathcal{H}$

Input : $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{R}[x]$

Output: $\mathcal{H}(f)$

begin
  $\mathcal{T} \leftarrow (d, |a_d|)$;
  $\mathcal{L} \leftarrow [\mathcal{T}]$;
  $l \leftarrow LineThrough(\ \mathcal{T},\ (0, \infty)\ )$;
  $\mathcal{H} \leftarrow -\infty$;
  for i *from* $d-1$ *to* 0 *by* -1 *do* **do**
    $\mathcal{P} \leftarrow (i, |a_i|)$;
    if a_i *is positive* **then**
      $(\mathcal{L}, \mathcal{T}, l) \leftarrow LowerHullUpdate(\mathcal{L}, \mathcal{P}, \mathcal{T}, l)$;
    else
      if $\mathcal{S}_{\mathcal{P},l[2]} < \mathcal{S}_{l[1],l[2]}$ `// ` $\mathcal{P}$ `lies below` l
      then
        $\mathcal{T} \leftarrow TangentPoint(L, \mathcal{P}, \mathcal{T})$;
        $l \leftarrow LineThrough(\ \mathcal{P},\ \mathcal{T})$;
        $\mathcal{H} \leftarrow \max\{\mathcal{H}, \mathcal{S}_{l[1],l[2]}\}$;
end

Remark 2.1. In [36], the point $\mathcal{T}$ and line l are not reset when $\mathcal{T}$ is removed from $\mathcal{L}$ (as we did when processing v_1 in the previous example, and as we do in Algorithm 1). This appears to a minor oversight which we correct here.

Theorem 2.2 (Melhorn, Ray, 2010 [36])**.** $B_H(f)$ can be computed in $\mathcal{O}(d)$ algebraic operations and comparisons using

$$B_H(f) = 2 \cdot Compute\mathcal{H}(f) \qquad \text{(Algorithm 3)}$$

Proof. We have already argued that that the total number of algebraic operations and comparisons required to process the positive points is $\mathcal{O}(d)$, since the Fast Convex Hull algorithm requires $\mathcal{O}(d)$ algebraic operations and comparisons. We also already argued that no edge can be traversed twice when processing negative points, due to Observation 2.1.3. In the Fast Convex Hull algorithm, $\mathcal{O}(d)$ total edges appear in the lower hull. Hence the negative points are processed in $\mathcal{O}(d)$ algebraic operations and comparisons as well. □

2.2 Root Separation Bounds of Univariate Polynomials

In this section, we discuss root separation bounds of univariate polynomials. The root separation of a polynomial is the minimum distance between every pair of roots. A root separation bound is a lower bound on the root separation. Root separation bounds are a fundamental tool in algorithmic mathematics, with numerous applications in science and engineering. For instance, they are employed in the study of topological properties of curves [31], exact geometric computation [32], algebraic number theory [19], sign evaluation of algebraic expressions [8], quantifier elimination [46], and real root isolation [52, 51].

First, we provide a formal definition of a root separation bound. Let $f = \sum_{i=0}^{d} a_i x^i = a_d \prod_{i=1}^{d} \prod(x - \alpha_i) \in \mathbb{C}[x]$.

Notation 2.2. $\Delta(f) = \min_{i \neq j} |\alpha_i - \alpha_j|$ is the *root separation* of f.

Definition 2.2. $B \in \mathbb{R}^+$ is a *root separation bound* if $B \leq \Delta(f)$.

Example 2.4. Consider again the example from the introduction. Let $f(x) = x^4 - 60x^3 + 1000x^2 - 8000x$. The roots of $f(x)$ are plotted in Figure 2.4. The lengths of the red line segments are the distances between the roots of $f(x)$. The root separation is the smallest of these distances. The root separation of $f(x)$ is $\sqrt{200}$, so any number $\leq \sqrt{200}$ is a root separation bound. □

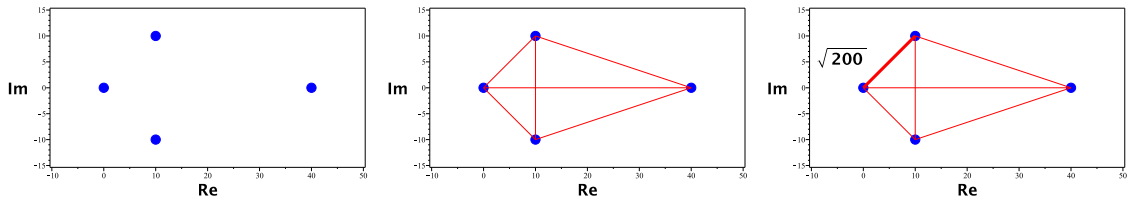

Figure 2.4: Roots of $f(x)$ (left), distances between roots (center), minimum separation highlighted (right)

Most root separation bounds are functions of the discriminant and polynomial norms.

Definition 2.3. The *discriminant* of f is

$$dis(f) = a_d^{2d-2} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

Some well known root separation bounds are listed below.

- Mahler-Mignotte, 1964 [33, 37]

$$B_{MM}(f) = \frac{\sqrt{3|dis(f)|}}{d^{d/2+1}||f||_2^{d-1}}$$

- Rump, 1979 [43]

$$B_{Rum}(f) = \frac{\min(1, |a_d|)^{d(\ln(d)+1)}|dis(f)|}{2^{d-1}d^{d-1}||f||_1^{d(\ln(d)+3)}}$$

- Mignotte, 1995 [40]

$$B_{Mig}(f) = \frac{\sqrt{6|dis(f)|}}{d^{d/2}((d-2)(2d-1))^{1/2}||f||_2^{d-1}}$$

- The DMM_1 bound [52] [3]

$$B_{DMM_1}(f) = \frac{|a_0|^2\sqrt{|dis(f)|}}{2^{d(d-1)/2-2}||f||_2^{d-1}}$$

There are many more root separation bounds in the literature (see [14, 5, 8, 37, 7, 44, 42, 39, 17] for more examples). Most have a structure similar to the bounds above.

In Chapter 4 of this thesis, we will present a framework for transforming a known root separation bound into a new improved root separation bound. We will choose to transform the Mahler bound. In the remainder of this section, we will re-derive the Mahler-Mignotte bound.

2.2.1 Derivation of the Mahler-Mignotte Bound

In this subsection, we re-derive the Mahler-Mignotte bound. We follow the commonly used convention of combining Mahler's original result from [33] and a result due to Mignotte [37]. Mignotte derived a bound on the *Mahler Measure* of a polynomial. This result is combined with Mahler's root separation bound (which depends on the Mahler measure of a polynomial) to derive a new root separation bound which depends on the discriminant, degree, and norm of a polynomial.

[3] In [52], an *aggregate* separation bound is presented. Aggregate separation bounds are generalizations of root separation bounds. An aggregate separation bound is a lower bound on products of factors of the form $|\alpha_i - \alpha_j|$. Here, we specialize the bound to the case when the product has a single factor. We also generalize the bound to the case when f has complex coefficients. This is done by using the lower bound $|\alpha_i| \geq |a_0|/\mathcal{M}(f)$, instead of $|\alpha_i| \geq \mathcal{M}(f)$ (which only applies to integer polynomials).

Definition 2.4. The *Mahler Measure* of f is

$$\mathcal{M}(f) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$$

We first re-derive Mignotte's bound on the Mahler measure. We require the following Lemma.

Lemma 2.2. Let $\gamma \in \mathbb{C}$. Then

$$||(x+\gamma)f||_2 = |\gamma| \cdot || \left(x + \frac{1}{\overline{\gamma}}\right) f||_2$$

Proof. Let $a_{-1} = a_{d+1} = 0$. To prove the claim, we will expand the squares of both sides of the above equation and observe that they are equal. Consider the following chain of equalities:

$$\begin{aligned} ||(x+\gamma)f||_2^2 &= \sum_{i=0}^{d+1} |a_{i-1} + \gamma a_i|^2 \\ &= \sum_{i=0}^{d+1} (a_{i-1} + \gamma a_i)\overline{(a_{i-1} + \gamma a_i)} \\ &= \sum_{i=0}^{d+1} (|a_{i-1}|^2 + \gamma a_i \overline{a_{i-1}} + \overline{\gamma} a_{i-1}\overline{a_i} + |\gamma|^2 |a_i|^2) \end{aligned} \tag{2.7}$$

Similarly, we have

$$\begin{aligned} |\gamma|^2 \cdot || \left(x + \frac{1}{\overline{\gamma}}\right) f||_2^2 &= \gamma\overline{\gamma} \cdot \sum_{i=0}^{d+1} \left| a_{i-1} + \frac{a_i}{\overline{\gamma}} \right|^2 \\ &= \gamma\overline{\gamma} \cdot \sum_{i=0}^{d+1} \left(a_{i-1} + \frac{a_i}{\overline{\gamma}}\right) \overline{\left(a_{i-1} + \frac{a_i}{\overline{\gamma}}\right)} \\ &= \sum_{i=0}^{d+1} \left(\overline{\gamma} a_{i-1} + a_i\right) \left(\gamma \overline{a_{i-1}} + \overline{a_i}\right) \\ &= \sum_{i=0}^{d+1} (|\gamma|^2 |a_{i-1}|^2 + \gamma a_i \overline{a_{i-1}} + \overline{\gamma} a_{i-1}\overline{a_i} + |a_i|^2) \\ &= \sum_{i=0}^{d+1} (|a_{i-1}|^2 + \gamma a_i \overline{a_{i-1}} + \overline{\gamma} a_{i-1}\overline{a_i} + |\gamma|^2 |a_i|^2) \quad \text{since } a_0 = a_{d+1} = 0 \end{aligned} \tag{2.8}$$

Combining (2.7) and (2.8) yields

$$||(x+\gamma)f||_2^2 = |\gamma|^2 \cdot || \left(x + \frac{1}{\overline{\gamma}}\right) f||_2^2$$

Taking the square root of both sides completes the proof. □

Theorem 2.3 (Mignotte, 1974 [37])**.** We have

$$\mathcal{M}(f) \leq ||f||_2$$

Proof. Without loss of generality, suppose that $0 \leq |\alpha_1| \leq \ldots |\alpha_k| \leq 1 < |\alpha_{k+1} \leq \ldots |\alpha_d|$. Define $h(x) = \prod_{i=1}^{k}(x-\alpha_i)$. We have

$$\begin{aligned}
||f||_2 =& |a_d| \cdot || \prod_{j=k+1}^{d} (x-\alpha_j) h||_2 \\
=& |a_d||\alpha_{k+1}| \cdot || \left(x - \frac{1}{\overline{\alpha_{k+1}}}\right) \prod_{j=k+2}^{d} (x-\alpha_j) h||_2 && \text{from Lemma 2.2} \\
=& |a_d||\alpha_{k+1}| \cdots |\alpha_d| \cdot || \prod_{j=k+1}^{d} \left(x - \frac{1}{\overline{\alpha_j}}\right) h||_2 && \text{from Lemma 2} \\
=& |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \cdot || \prod_{j=k+1}^{d} \left(x - \frac{1}{\overline{\alpha_j}}\right) h||_2 \\
=& \mathcal{M}(f) \cdot || \prod_{j=k+1}^{d} \left(x - \frac{1}{\overline{\alpha_j}}\right) h||_2 && (2.9)
\end{aligned}$$

Since h is monic, the polynomial $\prod_{j=k+1}^{d} \left(x - \frac{1}{\overline{\alpha_j}}\right) h$ is monic as well. Hence

$$|| \prod_{j=k+1}^{d} \left(x - \frac{1}{\overline{\alpha_j}}\right) h||_2 \geq 1 \qquad (2.10)$$

Combining (2.9) and (2.10) yields

$$\mathcal{M}(f) \leq ||f||_2$$

We have completed the proof of the Lemma. □

We will now re-derive Mahler's original bound: a root separation bound which depends on the Mahler measure of f.

Theorem 2.4 (Mahler, 1964 [33])**.** We have

$$\Delta(f) \geq \frac{\sqrt{3|dis(f)|}}{d^{(d+2)/2}\mathcal{M}(f)^{d-1}}$$

Proof. Without loss of generality, suppose that $|\alpha_1 - \alpha_2| = \Delta(f)$, with $|\alpha_1| \geq |\alpha_2|$. We will expand the expression for $|dis(f)|$ using the determinant of the Vandermonde matrix of $\{\alpha_1, \ldots, \alpha_d\}$.

$$\frac{|dis(f)|}{|a_d|^{2d-2}} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_d \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1} \end{vmatrix}^2$$

We can subtract the second column from the first without changing the value of the determinant:

$$\frac{|dis(f)|}{|a_d|^{2d-2}} = \begin{vmatrix} 0 & 1 & \cdots & 1 \\ \alpha_1 - \alpha_2 & \alpha_2 & \cdots & \alpha_d \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{d-1} - \alpha_2^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1} \end{vmatrix}^2$$

Hence

$$\frac{|dis(f)|}{|a_d|^{2d-2}} = |\alpha_1 - \alpha_2|^2 \begin{vmatrix} q_0 & 1 & \cdots & 1 \\ q_1 & \alpha_2 & \cdots & \alpha_d \\ \vdots & \vdots & \cdots & \vdots \\ q_{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1} \end{vmatrix}^2 \tag{2.11}$$

where $q_0 = 0$ and

$$q_h = \frac{\alpha_1^h - \alpha_2^h}{\alpha_1 - \alpha_2} = \sum_{j=0}^{h-1} \alpha_1^j \alpha_2^{h-j}. \tag{2.12}$$

Applying Hadamard's inequality to the right hand side of (2.11), we have

$$\frac{|dis(f)|}{|a_d|^{2d-2}} \leq |\alpha_1 - \alpha_2|^2 (|q_0|^2 + |q_1|^2 + \cdots + |q_{d-1}|^2) \prod_{i=2}^{d} p_i \tag{2.13}$$

where

$$p_i = \sum_{j=0}^{d-1} |\alpha_i|^{2j}.$$

Dividing both sides of (2.13) by $\mathcal{M}(f)^{2d-2}/|a_d|^{2d-2}$ yields

$$\frac{|dis(f)|}{\mathcal{M}(f)^{2d-2}} \leq |\alpha_1 - \alpha_2|^2 \frac{(|q_0|^2 + |q_1|^2 + \cdots + |q_{d-1}|^2)}{\max\{1, |\alpha_1|\}^{2d-2}} \prod_{i=2}^{d} \frac{p_i}{\max\{1, |\alpha_i|\}^{2d-2}} \tag{2.14}$$

For $i = 2, \ldots, d$ we have

$$\frac{p_i}{\max\{1, |\alpha_i|\}^{2d-2}} = \sum_{j=0}^{d-1} \left| \frac{\alpha_i^{2j}}{\max\{1, |\alpha_i|\}^{d-1}} \right|^2 \leq \sum_{j=0}^{d-1} 1 = d \tag{2.15}$$

We also have

$$\begin{aligned}
\frac{(|q_0|^2 + |q_1|^2 + \cdots + |q_{d-1}|^2)}{\max\{1, |\alpha_1|\}^{2d-2}} &= \sum_{h=0}^{d-1} \left| \frac{q_h}{\max\{1, |\alpha_1|\}^{d-1}} \right|^2 \\
&= \sum_{h=0}^{d-1} \left| \frac{\sum_{j=0}^{h-1} \alpha_1^j \alpha_2^{h-j}}{\max\{1, |\alpha_1|\}^{d-1}} \right|^2 && \text{from (2.12)} \\
&\leq \sum_{h=0}^{d-1} \left| \sum_{j=0}^{h-1} 1 \right|^2 && \text{since } |\alpha_1| \geq |\alpha_2| \text{ and } h \leq d \\
&= \sum_{h=0}^{d-1} h^2 && (2.16)
\end{aligned}$$

Combining (2.14),(2.15), and (2.16), we have

$$\frac{|dis(f)|}{\mathcal{M}(f)^{2d-2}} \leq |\alpha_r - \alpha_s|^2 d^{d-1} \sum_{h=0}^{d-1} h^2 \tag{2.17}$$

Note that

$$\sum_{h=0}^{d-1} h^2 = \frac{d(d-1)(2d-1)}{6} < \frac{d^3}{3} \tag{2.18}$$

Combining (2.17) and (2.18), we have

$$\frac{|dis(f)|}{\mathcal{M}(f)^{2d-2}} \leq |\alpha_1 - \alpha_2|^2 d^{d-1} \frac{d^3}{3} = |\alpha_1 - \alpha_2|^2 d^{d+2} \frac{1}{3}$$

Solving for $|\alpha_1 - \alpha_2|$ and recalling that $|\alpha_1 - \alpha_2| = \Delta(f)$, we have

$$\Delta(f) \geq \frac{\sqrt{3|dis(f)|}}{d^{(d+2)/2} \mathcal{M}(f)^{d-1}}$$

□

We now complete the derivation of the Mahler-Mignotte bound. Note that we present a separation bound which has a slightly different form than those at the beginning of this section. The bound in Proposition 2.1 depends on a parameter $k \geq 2$, and is a function of the $k-$norm of f.

Proposition 2.1. Let $k \in \mathbb{R}_+, k \geq 2$ and

$$B_{MM}(f) = \frac{\sqrt{|dis(f)|}}{||f||_k^{d-1}} P_k(d)$$

where

$$P_k(d) = \frac{\sqrt{3}}{d^{d/2+1}(d+1)^{(\frac{1}{2}-\frac{1}{k})(d-1)}}$$

Then $\Delta(f) \geq B_{MM,k}$.

Proof. When $k = 2$, we apply Theorem 2.3 to the expression in Theorem 2.4. For $k \geq 2$, we then apply the well known norm inequality

$$||f||_2 \leq (d+1)^{(\frac{1}{2}-\frac{1}{k})} ||f||_k$$

□

2.3 Root Separation Bounds of Polynomial Systems

In this section, we discuss root separation bounds of polynomial systems. The root separation of a polynomial system is the minimum distance between every pair of roots. A root separation bound is a lower bound on the root separation. The study of root separation bounds on polynomial systems is more recent than root separation bounds on univariate polynomials. Many applications arise when generalizing algorithms for univariate polynomials; for example, subdivision algorithms of polynomials systems can be analyzed with root separation bounds [18, 34].

First, we will extend the definition of a root separation bound from the previous section to polynomial systems. Let $F = (f_1, \ldots, f_n) \in \mathbb{C}^n[x_1, \ldots, x_n]$ be a zero dimensional polynomial system with no multiple roots. Let $\{\alpha_i\}$ denote the roots of F.

Notation 2.3. $\Delta(F) = \min_{i \neq j} ||\alpha_i - \alpha_j||_2$ is the *root separation* of F.

Definition 2.5. $B \in \mathbb{R}^+$ is a *root separation bound* if $B \leq \Delta(F)$.

Example 2.5. Let $F = (f_1, f_2)$, where

$$f_1 = x_1^2 + x_2^2 - 100$$
$$f_2 = x_1^2 - x_2^2 - 25$$

The roots of F are plotted in Figure 2.5. Note that the root separation $\Delta(F)$ is $\sqrt{150}$. Hence, any number less than or equal to $\sqrt{150}$ is a root separation bound. □

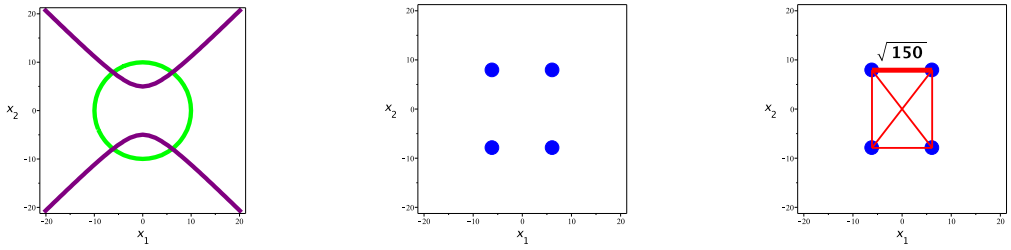

Figure 2.5: The curves $f_1 = 0$ and $f_2 = 0$ (Left), the roots of F (center), with root separation highlighted (right).

The study of root separation bounds on polynomial systems is relatively new. As a consequence, we cannot present a list of efficiently computable separation bound formulas from the literature (although there are bounds which are defined implicitly, eg [15]). We will concern ourselves mainly with the Emiris- Mourrain-Tsigaridas bound.

- Emiris, Mourrain, and Tsigaridas, 2010 [18] [4]

$$B_{EMT}(F) = \frac{\sqrt{|dis(T_{f_0})|}}{(\prod_{i=1}^{n} ||f_i||^{M_i})^{D-1}} P(d_1, \ldots, d_n, n)$$

where

$$P(d_1, \ldots, d_n, n) = \frac{\sqrt{3}}{D^{D/2+1} \cdot n^{1/2} C \cdot \left(\sqrt{D+1}(n+1)^D C^D \prod_{i=1}^{n} \binom{d_i+n}{d_i}^{M_i} \right)^{D-1}}$$

$$T_{f_0} = \text{the resultant of } (f_0, f_1, \ldots, f_n) \text{ which eliminates } \{x_1, \ldots, x_n\}$$

$$f_0 = \text{a separating element in the set}$$

$$\left\{ u - x_1 - ix_2 - \cdots - i^{n-1}x_n : 0 \leq i \leq (n-1)\binom{D}{2} \right\}$$

$$M_i = \prod_{j \neq i} d_j$$

$$C = \left((n-1)\binom{D}{2} \right)^{n-1}$$

In Chapter 5 of this thesis, we extend the framework of the previous chapter to transform a known root separation bound on polynomial systems. We will choose to transform the Emiris-Mourrain-Tsigaridas bound. In the remainder of this section, we re-derive the Emiris-Mourrain-Tsigaridas bound.

2.3.1 Derivation of the Emiris-Mourrain-Tsigaridas Bound

In this section, we re-derive the Emiris-Mourrain-Tsigaridas bound. We will use the following overall strategy:

1. Construct a $u-$resultant $T(u)$. This is the resultant of F and a specially chosen $f_0 \in \mathbb{C}[u, x_1, \ldots, x_n]$ which eliminates $\{x_1, \ldots, x_n\}$ We choose f_0 so that $T(u)$ is square-free.
2. Relate the root separation of F and the root separation of T.
3. Apply the Mahler bound to T.
4. Combine steps 2 and 3 to construct the new root separation bound.

In [18], the authors apply the univariate root separation bound DMM_1 (Theorem 1 in that paper) in Step 3. Unfortunately Theorem 1 as stated has a slight error; it cannot be applied to

[4] The bound presented here is a slight modification of the bound in [18]. We perform the modification to correct a slight error in the original bound. See the next section for more details.

non-integer polynomials. To derive the multivariate root separation bound, we need to apply a univariate root separation bound which can be applied to complex polynomials. One strategy is to modify DMM_1 so that it applies to complex polynomials. Another strategy is to apply a different bound; here, we simply apply $B_{Mah,\infty}$ to T.

Before constructing the $u-$resultant $T(u)$, we require the following definition.

Definition 2.6. Let $f_0 = u - r_1x_1 - \cdots - r_nx_n \in \mathbb{C}[u, x_1, \ldots, x_n]$. We say f_0 is a *separating element* of F if the mapping

$$\begin{aligned} V(F) &\to \mathbb{C} \\ \beta &\mapsto r_1\beta_1 + \cdots + r_n\beta_n \end{aligned}$$

is injective.

If f_0 is a separating element of F, then the polynomial $T(u)$ is square-free. We illustrate the definition and square-free property by a simple example.

Example 2.6. Let F be the same as in Example 2.5. Consider

$$f_0 = u - x_1$$

In the left plot Figure 2.6, we project every point in $\mathbb{R}_2$ onto its x_1 coordinate (the red line). The projections of the four roots are the red dots. We can clearly see from this projection that the mapping $\beta \mapsto \beta_1$ is not injective on the roots of F. Hence f_0 is not a separating element of F. Now consider the u-resultant

$$T(u) = res(f_0, f_1, f_2) \text{ which eliminates } x_1 \text{ and } x_2$$

It is simple to verify that $T(u) = (2u^2 - 5)^2$. Clearly this polynomial is not square-free. Hence any root separation on $T(u)$ will trivially be zero.

Now consider the polynomial

$$f_0 = u - x_1 - x_2$$

In the right plot of Figure 2.6, we project every point in $\mathbb{R}_2$ onto its $x_1 + x_2$ value (the red line). The projections of the four roots are the red dots. We can clearly see from this projection that the mapping $\beta \mapsto \beta_1 + \beta_2$ is injective on the roots of F. Hence f_0 is a separating element of F. Now consider the same $u-$resultant construction as before, with the new choice of f_0. We have

$$T(u) = 4u^2 - 800u^2 + 2500$$

We compute

$$dis(T) \;=\; 5.76 \times 10^{16} \;\neq\; 0$$

Hence $T(u)$ is square-free, and a root separation bound on $T(u)$ will not be trivially 0. □

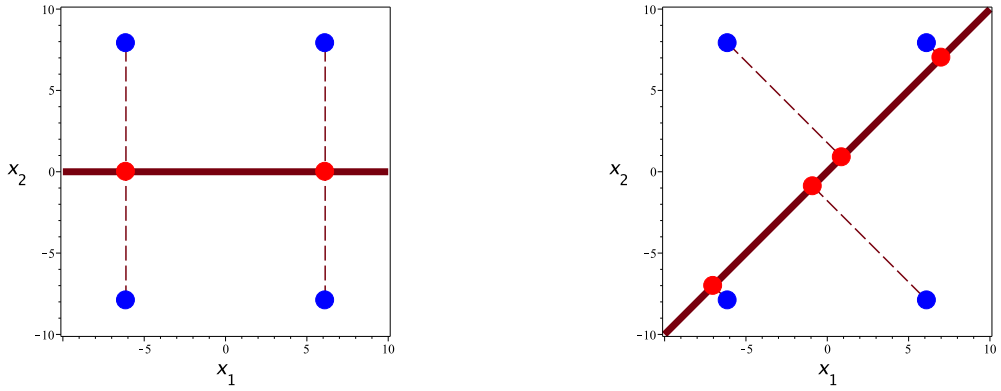

Figure 2.6: Not a separating element (left), separating element (right)

Following [18], we will now present a well known set which has at least one separating element.

Lemma 2.3 (Proposition 6 in [18])**.** The set

$$\left\{ u - x_1 - ix_2 - \cdots - i^{n-1}x_n : 0 \leq i \leq (n-1)\binom{D}{2} \right\}$$

has at least one separating element.

The construction of the set above is motivated by the simple observation that there can be at most $(n-1)\binom{D}{2}$ directions $(r_1, \ldots, r_n)$ which yield a non-injective projection. The set is also chosen so that all polynomials in the set have integer coefficients.

Example 2.7. In the above example, f_0 is the element of $\mathcal{F}$ defined by $i = 1$.

To relate the root separation of F and the univariate polynomial T, we require the Cauchy-Schwartz inequality.

Lemma 2.4 (Cachy-Schwartz Inequality)**.** Let $a \in \mathbb{C}^n$ and $b \in \mathbb{C}^n$. Then

$$|\overline{a_1}b_1 + \cdots + \overline{a_n}b_n|^2 \leq (|a_1|^2 + \cdot + |a_n|^2)(|b_1|^2 + \cdots + |b_n|^2)$$

Lemma 2.5. Let $f_0 = u - r_1x_1 - \cdots - r_nx_n \in \mathbb{R}[u, x_1, \ldots, x_n]$. Let $T_{f_0}(u)$ denote the resultant of F and f_0 which eliminates $x_1, \ldots, x_n$. Then

$$\Delta(F) \geq \frac{\Delta(T)}{\left(r_1^2 + \cdots + r_n^2\right)^{1/2}}$$

Proof. Let $\{\gamma\}_{i=1}^{D}$ denote the roots of T. Without loss of generality, assume that

$$\gamma_i = r_1\alpha_{i,1} + \cdots + r_n\alpha_{i,n} \tag{2.19}$$

$$\Delta(F) = ||\alpha_1 - \alpha_2||_2 \tag{2.20}$$

We have

$$\begin{aligned}
|\gamma_1 - \gamma_2|^2 &= |(r_1\alpha_{1,1} + \cdots + r_n\alpha_{1,n}) - (r_1\alpha_{2,1} + \cdots + r_n\alpha_{2,n})| && \text{from (2.19)} \\
&= |r_1(\alpha_{1,1} - \alpha_{2,1}) + \cdots + r_n(\alpha_{1,n} - \alpha_{2,n})| \\
&\leq \left(r_1^2 + \cdots + r_n^2\right)\left((\alpha_{1,1} - \alpha_{2,1})^2 + \cdots + (\alpha_{1,n} - \alpha_{2,n})^2\right) && \text{from Lemma 2.4} \\
&= \left(r_1^2 + \cdots + r_n^2\right)||\alpha_1 - \alpha_2||_2^2 \\
&= \left(r_1^2 + \cdots + r_n^2\right)^2 \Delta(F)^2 && \text{from (2.20)}
\end{aligned}$$

Rearranging and solving for $\Delta(F)$ yields

$$\begin{aligned}
\Delta(F) &\geq \frac{|\gamma_1 - \gamma_2|}{\left(r_1^2 + \cdots + r_n^2\right)^{1/2}} \\
&\geq \frac{\Delta(T)}{\left(r_1^2 + \cdots + r_n^2\right)^{1/2}}
\end{aligned}$$

We have completed the proof of the Lemma. □

Lemma 2.6. Let $f_0 \in \mathcal{F}$ and T_{f_0} the resultant of (f_0, F) which eliminates $x_1, \ldots, x_n$. Then

$$||T_{f_0}||_\infty \leq \prod_{i=1}^{n} ||f_i||_\infty^{M_i} C^D (n+1)^D \prod_{i=1}^{n} \binom{n + d_i}{d_i}^{M_i}$$

Proof. For $i = 0, \ldots, n$, $T_{f_0}(u)$ is homogeneous of degree

$$\begin{aligned}
d_0d_1d_2 \ldots d_{i-1}d_{i+1} \cdots d_n &= d_1d_2 \ldots d_{i-1}d_{i+1} \cdots d_n && \text{since } d_0 = 1 \\
&= M_i
\end{aligned}$$

in the coefficients of f_i. It is well known that $T_{f_0}(u)$ is a homogenous integer polynomial in the

coefficients of (F, f_0) with degree D in u. We can write

$$T_{f_0}(u) = \cdots + \left(\rho_k r_k^{D-k} \prod_{i=1}^{n} c_{i,k}^{M_i} \right) \cdot u^k + \cdots \tag{2.21}$$

where $\rho_k \in \mathbb{Z}$, $c_{i,k}^{M_i}$ is a monomial in the coefficients of f_i of total degree M_i, and r_k^{D-k} is a monomial in the coefficients of f_0 with total degree $D-k$. Since

$$c_{i,k}^{M_i} = a_1^{e_1} \cdots a_r^{e_r}$$

with all a_j coefficients of f_i and $e_1 + \cdots + e_r = M_i$, we have

$$\begin{aligned} c_{i,k}^{M_i} &= a_1^{e_1} \cdots a_r^{e_r} \\ &\leq ||f_i||_\infty^{e_1} \cdots ||f_i||_\infty^{e_r} \\ &= ||f_i||_\infty^{e_1 + \cdots + r_r} \\ &= ||f_i||_\infty^{M_i} \end{aligned}$$

Hence

$$\prod_{i=1}^{n} c_{i,k}^{M_i} \leq \prod_{i=1}^{n} ||f_i||_\infty^{M_i} \tag{2.22}$$

Under identical reasoning, we have

$$|r_k|^{D-k} \leq ||f_0||_\infty^{D-k} \leq C^{D-k} \tag{2.23}$$

From Theorem 1.1 of [48], we have

$$\max |\rho_k| \leq \prod_{i=0}^{n} (\#\text{ of monomials of degree } d_i)^{M_i} \tag{2.24}$$

Since $f_0 \in \mathcal{F}$, the number of monomials of degree d_0 is $(n+1)$. Note also that $M_0 = d_1 \cdots d_n = D$. Hence

$$(\#\text{ of monomials of degree } d_0)^{M_0} = (n+1)^D \tag{2.25}$$

For $i \geq 0$, we have

$$(\#\text{ of monomials of degree } d_i)^{M_i} \leq \binom{n+d_i}{d_i}^{M_i} \tag{2.26}$$

Combining (2.24), (2.25), and (2.26), we have

$$\max|\rho_k| \leq (n+1)^D \prod_{i=1}^{n} \binom{n+d_i}{d_i}^{M_i} \tag{2.27}$$

Now we bound the norm of T_{f_0}. We have

$$\begin{aligned}
||T_{f_0}||_\infty &= \max_{0\leq k\leq D} \left| \rho_k r_k^{D-k} \prod_{i=1}^{n} c_{i,k}^{M_i} \right| \\
&\leq \max_{0\leq k\leq D} \left| \rho_k r_k^{D-k} \prod_{i=1}^{n} ||f_i||_\infty^{M_i} \right| && \text{from (2.22)} \\
&= \prod_{i=1}^{n} ||f_i||_\infty^{M_i} \max_{0\leq k\leq D} \left| \rho_k r_k^{D-k} \right| \\
&\leq \prod_{i=1}^{n} ||f_i||_\infty^{M_i} \max_{0\leq k\leq D} \left| \rho_k C^{D-k} \right| && \text{from (2.23)} \\
&= \prod_{i=1}^{n} ||f_i||_\infty^{M_i} C^D \max_{0\leq k\leq D} |\rho_k| \\
&\leq \prod_{i=1}^{n} ||f_i||_\infty^{M_i} C^D \max_{0\leq k\leq D} \left| (n+1)^D \prod_{i=1}^{n} \binom{n+d_i}{d_i}^{M_i} \right| && \text{from (2.27)} \\
&= \prod_{i=1}^{n} ||f_i||_\infty^{M_i} C^D (n+1)^D \prod_{i=1}^{n} \binom{n+d_i}{d_i}^{M_i}
\end{aligned}$$

We have proved the Lemma.

□

Theorem 2.5 (Emiris, Mourrain, and Tsigaridas, 2010 [18])**.** Let

$$B(F) = \frac{\sqrt{|dis(T_{f_0})|}}{\left(\prod_{i=1}^{n} ||f_i||^{M_i}\right)^{D-1}} P(d_1, \ldots, d_n, n)$$

where

$$\begin{aligned}
P(d_1, \ldots, d_n, n) &= \frac{\sqrt{3}}{D^{D/2+1} \cdot n^{1/2} C \cdot \left(\sqrt{D+1}(n+1)^D C^D \prod_{i=1}^{n} \binom{d_i+n}{d_i}^{M_i} \right)^{D-1}} \\
T_{f_0} &= \text{the resultant of } (f_0, f_1, \ldots, f_n) \text{ which eliminates } \{x_1, \ldots, x_n\} \\
f_0 &= \text{a separating element in the set} \\
&\qquad \left\{ u - x_1 - ix_2 - \cdots - i^{n-1}x_n : 0 \leq i \leq (n-1)\binom{D}{2} \right\}
\end{aligned}$$

$$M_i = \prod_{j \neq i} d_j$$
$$C = \left((n-1) \binom{D}{2} \right)^{n-1}$$

Then $\Delta(F) \geq B(F)$.

Proof. Clearly, we can write

$$f_0 = u - r_1 x_1 - \cdots - r_n x_n \tag{2.28}$$

Since $f_0 \in \mathcal{F}$, we have

$$|r_k| \leq C, \quad k = 1 \cdots, n \tag{2.29}$$

Combining (2.28), (2.29), and Lemma 2.5, we have

$$\Delta(F) \geq \frac{\Delta(T_{f_0})}{\left(r_1^2 + \cdots + r_n^2\right)^{1/2}} \geq \frac{\Delta(T_{f_0})}{\left(n \cdot C^2\right)^{1/2}} = \frac{\Delta(T_{f_0})}{n^{1/2} \cdot C} \tag{2.30}$$

We now apply the bound $B_{Mah,\infty}$ to T_{f_0}. Recall that the degree of T_{f_0} is D. We have

$$\begin{aligned}
\Delta(T_{f_0}) &\geq B_{Mah,\infty}(T_{f_0}) \\
&= \frac{\sqrt{3|dis(T_{f_0})|}}{D^{D/2+1}\sqrt{D+1}^{D-1}||T_{f_0}||_\infty^{D-1}} \\
&\geq \frac{\sqrt{3|dis(T_{f_0})|}}{D^{D/2+1}\sqrt{D+1}^{D-1}\left(\prod_{i=1}^n ||f_i||_\infty^{M_i} C^D (n+1)^D \prod_{i=1}^n \binom{n+d_i}{d_i}^{M_i}\right)^{D-1}}
\end{aligned} \tag{2.31}$$

where the last inequality is from Lemma 2.6. Combining (2.30) and (2.31) yields

$$\begin{aligned}
\Delta(F) &\geq \frac{\sqrt{3|dis(T_{f_0})|}}{D^{D/2+1}\sqrt{D+1}^{D-1} \cdot n^{1/2} C \cdot \left(\prod_{i=1}^n ||f_i||_\infty^{M_i} C^D (n+1)^D \prod_{i=1}^n \binom{n+d_i}{d_i}^{M_i}\right)^{D-1}} \\
&= \frac{\sqrt{|dis(T_{f_0})|}}{\left(\prod_{i=1}^n ||f_i||^{M_i}\right)^{D-1}} P(d_1, \ldots, d_n, n) \\
&= B(F)
\end{aligned}$$

We have completed the proof of the theorem. □

Chapter 3

Positive Root Bounds of Univariate Polynomials

Introduction

In this chapter, we investigate the *quality* of known positive root bounds. Of course, every positive root bound over-estimates the largest real root. Higher quality means that the relative over-estimation (the ratio of the positive root bound and the largest positive root) is smaller. We report three findings.

1. We show that most known positive root bounds can be *arbitrarily bad*; that is, the relative over-estimation can approach infinity, even when the degree and the coefficient size are fixed. A precise statement is given in Theorem 3.1. Contrast this result with similar results on root bounds (upper bounds on the magnitude of the roots): it has been shown that a root bound due to Fujiwara over-estimates the largest magnitude by at most twice the degree [54].

   In fact, we prove a more general result: we show that every positive root bound which is also an *absolute positiveness bound* (a bound on the largest positive root *and* the positive roots of the derivatives, see Definition 3.1) can be arbitrarily bad. All positive root bounds listed in Chapter 2 are absolute positiveness bounds, as well as every positive root bound derived in the framework in [6]. It also appears that every positive root bound derived in the framework in [2] is an absolute positiveness bound, although we do not have a proof.

2. We show that when the number of sign variations is the same as the number of positive roots, the relative over-estimation of the Hong Bound (B_H) is at most *linear* in the degree, no matter what the coefficient size is. A precise statement is given in Theorem 3.2.

The motivation for considering number of sign variations is as follows. Theorem 3.1 is a consequence of the fact that for fixed degree and coefficient size, the largest positive root of a polynomial can be arbitrarily smaller than the largest root of its derivatives. Therefore one might wonder if the quality is better when the largest positive root bounds the roots of the derivatives also. One natural case when this happens is when Descartes Rule of Signs is exact (Lemma 3.5).

It is immediate from an example in Theorem 5.3 of [22] that the relative over-estimations of B_L, B_C, and B_K (presented in Chapter 2) can approach infinity, even when the degree is fixed and when the number of sign variations is the same as the number of positive roots. The proof strategy for Theorem 3.2 can be easily adapted to show that the relative over-estimation of every positive root bound in the framework in [6] is at most linear in the degree. It also immediate that there exists at least one positive root bound (namely B_K) in the framework from [2] whose relative over-estimation can approach infinity.

3. We show that when the number of sign variations is one, the relative over-estimation of B_H is at most *constant*, in particular 4, no matter what the degree and the coefficient size are. A precise statement is given in Theorem 3.3.

   It is again immediate from an example in Theorem 5.3 of [22] that the relative over-estimations of B_L, B_C, and B_K can approach infinity, even when the degree is fixed and when the number of sign variations is one. It is not clear if there exists a constant bound on the relative over-estimation for every positive root bound in the framework from [6]. It also immediate that there exists at least one positive root bound (namely B_K) in the framework from [2] whose relative over-estimation can approach infinity.

3.1 Main Results

In this section, we will precisely state the main results of this chapter. Let $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{R}[x]$. We will assume the following throughout the chapter.

Assumption 3.1.

1. f has a positive leading coefficient.
2. f has at least one positive root.

We will use the following notations.

Notation 3.1.

$$
\begin{aligned}
||f|| &= \max_{0 \le i < d-1} \frac{|a_i|}{|a_d|} \\
\mathcal{V}(f) &= \text{the number of sign variations of } f \\
\mathcal{C}(f) &= \text{the number of positive roots of } f\text{, counting multiplicities} \\
x^*(f) &= \text{the largest positive root of } f \\
B(f) &= \text{an upper bound on } x^*(f) \\
\mathcal{R}_B(f) &= \frac{B(f)}{x^*(f)}
\end{aligned}
$$

Remark 3.1. From Descartes Rule of Signs, we have $\mathcal{V}(f) \geq \mathcal{C}(f)$ and $\mathcal{V}(f) \equiv \mathcal{C}(f) \mod 2$. The symbol B stands for a positive root bound. The symbol $\mathcal{R}$ stands for "relative over-estimation". For every positive root bound B, we obviously have $\mathcal{R}_B(f) \geq 1$.

Definition 3.1 (Absolute positiveness bound [22])**.** $B : \mathbb{R}[x] \to \mathbb{R}_+$ is an *absolute positiveness bound* if

$$B(f) \ \geq \ a^*(f)$$

where $a^*(f)$ is the *threshold of absolute positiveness*

$$a^*(f) = \max \left\{ \alpha \in \mathbb{R} : \exists i \in [0, \ldots, d-1] \quad f^{(i)}(\alpha) = 0 \right\}$$

First we show that every *absolute positiveness bound* can be arbitrarily bad.

Theorem 3.1 (Over-Estimation is unbounded)**.** Let $B : \mathbb{R}[x] \to \mathbb{R}_+$ be an absolute positiveness bound. Let $d \geq 4$ and $b > 0$. Then

$$\sup_{\substack{\deg(f)=d \\ ||f||=b}} \mathcal{R}_B(f) = \infty$$

Next we show that when the number of sign variations is equal to the number of positive roots, the relative over-estimation of B_H is at most *linear* in the degree.

Theorem 3.2 (Over-Estimation when Descartes Rule of Signs is exact)**.** We have

$$\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=\mathcal{C}(f)}} R_{B_H}(f) \leq \frac{2d}{\ln(2)}$$

Finally we show that when the number of sign variations is one, the relative over-estimation of B_H is at most *constant*, in particular 4.

Theorem 3.3 (Over-Estimation when there is a single sign variation)**.** We have

$$\sup_{\mathcal{V}(f)=1} \mathcal{R}_{B_H}(f) \;=\; 4$$

Example 3.1. We will illustrate the result by a simple example.

$$\begin{aligned}
f &= x^3 + 9x^2 - 3x - 6 \\
\mathcal{V}(f) &= 1 \\
x^*(f) &\approx 0.94 \\
B_H(f) &= 2 \max_{q\in\{0,1\}} \min_{p\in\{2,3\}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}} \\
&= 2 \max\left\{\min\left\{\left(\frac{6}{9}\right)^{\frac{1}{2-0}}, \left(\frac{6}{1}\right)^{\frac{1}{3-0}}\right\}, \min\left\{\left(\frac{3}{9}\right)^{\frac{1}{2-1}}, \left(\frac{3}{1}\right)^{\frac{1}{3-1}}\right\}\right\} \\
&\approx 1.63 \\
\mathcal{R}_{B_H}(f) &= \frac{B(f)}{x^*(f)} \approx 1.73
\end{aligned}$$

Thus we have

$$\mathcal{R}_{B_H}(f) \approx 1.73 \;\;\leq\;\; 4,$$

confirming Theorem 3.3. □

Remark 3.2. It turns out that when the sign variation is fixed at 1, the *index* at which the sign variation occurs affects the average value of the relative over-estimation. We discuss this phenomena in Appendix 3.B.

Remark 3.3. What if the number of sign variations is greater than one and not the same as the number of positive roots? It turns out that the relative over-estimation of every absolute positiveness bound can approach infinity even when the degree is fixed. Precisely, for every absolute positiveness bound B and $k > 1$, one can show that

$$\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=k \\ \mathcal{C}(f)\neq\mathcal{V}(f)}} \mathcal{R}_B(f) = \infty$$

We include a proof of this statement in Appendix 3.C.

3.2 Proof of Theorem "Over-Estimation is unbounded"

In this section, we will prove Theorem 3.1. Let B be an absolute positiveness bound. Let $d \geq 4, b > 0$ be fixed. We will exploit the following polynomial parameterized by c:

$$f_c = \begin{cases} x^{d-4}(x-c)(x+c)\left((x-\frac{b}{2})^2 + c^2\right) & b < 4 \\ x^{d-4}(x-c)(x+c)\left((x-\sqrt{b})^2 + c^2\right) & b \geq 4 \end{cases}$$
$$= \begin{cases} x^d - bx^{d-1} + \frac{b^2}{4}x^{d-2} + c^2 bx^{d-3} - c^2\left(\frac{b^2}{4} + c^2\right)x^{d-4} & b < 4 \\ x^d - 2\sqrt{b}x^{d-1} + bx^{d-2} + c^2 2\sqrt{b}x^{d-3} - c^2\left(b + c^2\right)x^{d-4} & b \geq 4 \end{cases}$$

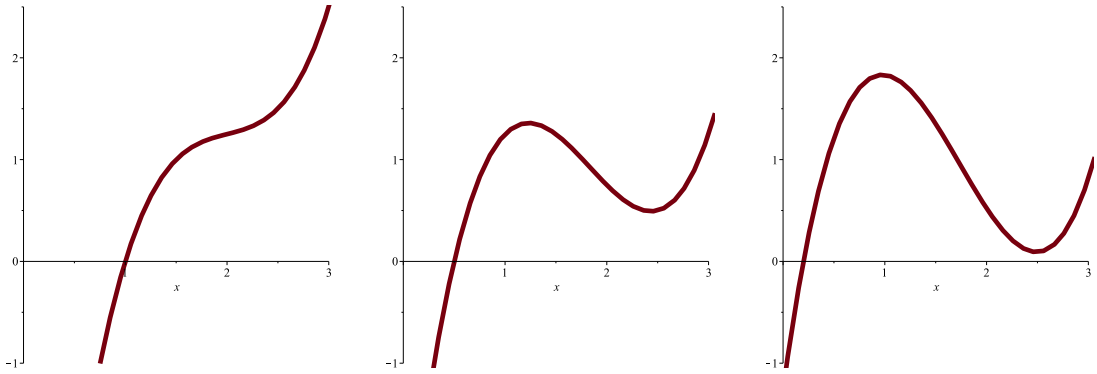

Figure 3.1: Plot of f_c for $b = 5$ and $c = 1$ (left), $c = .5$ (middle), $c = .2$ (right)

We will use two key Lemmas.

Lemma 3.1. We have

1. f_c satisfies Assumption 3.1.
2. $\deg(f_c) = d$.
3. $\exists \overline{c} > 0 \quad \forall c \in (0, \overline{c}) \quad ||f_c|| = b$.

Proof. We prove them one by one.

1. Obvious.

2. Obvious.

3. Suppose $b < 4$. Let $\overline{c}$ be any positive number such that

$$\overline{c} < 1 \tag{3.1}$$

and

$$\overline{c}^2 \left(\frac{b^2}{4} + \overline{c}^2 \right) < b \tag{3.2}$$

Such a $\overline{c}$ exists because the left hand side of (3.2) can be made arbitrarily small for fixed b. Then for all $c \in (0, \overline{c})$, we have

$$\begin{aligned}
||f_c|| &= \max \left\{ b, \frac{b^2}{4}, c^2 b, c^2 \left(\frac{b^2}{4} + c^2 \right) \right\} \\
&= \max \left\{ b, c^2 b, c^2 \left(\frac{b^2}{4} + c^2 \right) \right\} && \text{since } \frac{b}{4} < 1 \\
&= \max \left\{ b, c^2 \left(\frac{b^2}{4} + c^2 \right) \right\} && \text{from (3.1)} \\
&= b && \text{from (3.2)}
\end{aligned}$$

Suppose $b \geq 4$. Let $\overline{c}$ be any positive number such that

$$\overline{c} < 1 \tag{3.3}$$

and

$$\overline{c}^2 \cdot (b + \overline{c}^2) < b \tag{3.4}$$

Such a $\overline{c}$ exists because the right hand side of (3.4) can be made arbitrarily small for fixed b. Then for all $0 < c < \overline{c}$, we have

$$\begin{aligned}
||f_c|| &= \max \left\{ 2\sqrt{b}, b, c^2 \cdot 2\sqrt{b}, c^2 \cdot (b + c^2) \right\} \\
&= \max \left\{ 2\sqrt{b}, b, c^2 \cdot (b + c^2) \right\} && \text{from (3.3)} \\
&= \max \left\{ b, c^2 \cdot (b + c^2) \right\} && \text{since } 2 < \sqrt{b} \\
&= b && \text{from (3.4)}
\end{aligned}$$

We have proved the Lemma. □

Lemma 3.2. There exists $\omega > 0$ such that for all $c > 0$

1. $x^*(f_c) = c$

2. $B(f_c) \geq \omega$

Proof. We prove them one by one.

1. Obvious.

2. Suppose $b < 4$. Let $\omega = \frac{b}{d}$ and $c > 0$. We have

$$f_c^{(d-1)} = (d)(d-1)\cdots(2)\cdot x - (d-1)(d-2)\cdots(1)\cdot b$$

Hence $x^*(f_c)^{(d-1)} = \frac{b}{d} = \omega$. Since B is an absolute positiveness bound, we have

$$B(f_c) \geq x^*(f_c)^{(d-1)} = \omega$$

Suppose $b \geq 4$. Let $\omega = \frac{2\sqrt{b}}{d}$ and $c > 0$. We have

$$f_c^{(d-1)} = (d)(d-1)\cdots(2)\cdot x - (d-1)(d-2)\cdots(1)\cdot 2\sqrt{b}$$

Hence $x^*(f_c)^{(d-1)} = \frac{2\sqrt{b}}{d} = \omega$. Since B is an absolute positiveness bound, we have

$$B(f_c) \geq x^*(f_c)^{(d-1)} = \omega$$

We have proved the Lemma. □

Proof of Theorem 3.1. Let $\overline{c}, \omega$ be defined as in Lemmas 3.1 and 3.2. We have

$$\begin{aligned}
\sup_{\substack{\deg(f)=d \\ ||f||=b}} \mathcal{R}_B(f) &= \sup_{\substack{\deg(f)=d \\ ||f||=b}} \frac{B(f)}{x^*(f)} \\
&\geq \sup_{\substack{f_c \\ 0<c<\overline{c}}} \frac{B(f_c)}{x^*(f_c)} && \text{from Lemma 3.1} \\
&\geq \lim_{c\to 0} \frac{B(f_c)}{x^*(f_c)} \\
&= \lim_{c\to 0} \frac{B(f_c)}{c} && \text{from Lemma 3.2} \\
&\geq \lim_{c\to 0} \frac{\omega}{c} && \text{from Lemma 3.2} \\
&= \infty
\end{aligned}$$

We have proved Theorem 3.1. □

3.3 Proof of Theorem "Over-Estimation when Descartes Rule of Signs is exact"

In this section, we prove Theorem 3.2. Essentially, we prove Theorem 3.2 by showing that if $\mathcal{V}(f) = \mathcal{C}(f)$, then $a^*(f) = x^*(f)$. We then use Theorem 2.3 of [22] to complete the proof. We break the proof into several Lemmas for clarity.

Lemma 3.3. If

$$\mathcal{V}(f) = \mathcal{C}(f)$$

then

$$\mathcal{V}(f') = \mathcal{C}(f')$$

Proof. From Descartes Rule of Signs

$$\mathcal{C}(f') \leq \mathcal{V}(f') \tag{3.5}$$

and

$$\mathcal{C}(f') = \mathcal{V}(f') \mod 2 \tag{3.6}$$

From repeated application of Rolle's Theorem, f' has at least $\mathcal{C}(f) - 1$ positive roots. Hence

$$\begin{aligned} \mathcal{C}(f') &\geq \mathcal{C}(f) - 1 \\ &= \mathcal{V}(f) - 1 \qquad \text{since } \mathcal{C}(f) = \mathcal{V}(f) \end{aligned} \tag{3.7}$$

Combining (3.5) and (3.7), we have

$$\mathcal{V}(f) - 1 \leq \mathcal{C}(f') \leq \mathcal{V}(f') \tag{3.8}$$

Clearly,

$$\mathcal{V}(f') \leq \mathcal{V}(f) \tag{3.9}$$

Combining (3.8) and (3.9), we have

$$\mathcal{V}(f) - 1 \leq \mathcal{C}(f') \leq \mathcal{V}(f') \leq \mathcal{V}(f) \tag{3.10}$$

Combining (3.6) and (3.10), we have

$$\mathcal{C}(f') = \mathcal{V}(f')$$

We have proved the Lemma. □

Lemma 3.4. If

$$\mathcal{V}(f) = \mathcal{C}(f)$$

and f' has a positive root, then

$$x^*(f') \leq x^*(f)$$

Proof. Let $k = \mathcal{V}(f)$. Without loss of generality, suppose that the positive roots of f are ordered so that

$$\alpha_1 \leq \cdots \leq \alpha_k$$

Suppose that $x^*(f') > x^*(f) = \alpha_k$. We will derive a contradiction. From repeated application of Rolle's Theorem, f' has $k-1$ roots in the interval $[\alpha_1, \ldots, \alpha_k]$. Since f' has at most k roots by Descartes Rule of Signs and $x^*(f') > \alpha_k$, f' has k roots

$$\beta_1 \leq \ldots \beta_{k-1} \leq \beta_k$$

where $\beta_{k-1} \leq \alpha_k < \beta_k$. Since f has positive leading coefficient and α_k is the largest root of f,

$$f \text{ is strictly positive on } (\alpha_k, \infty) \tag{3.11}$$

By identical reasoning

$$f' \text{ is strictly positive on } (\beta_k, \infty) \tag{3.12}$$

Since β_k is not a double root of f', it follows that f' is strictly negative on the interval (β_{k-1}, β_k). In particular,

$$f' \text{ is strictly negative on the interval } (\alpha_k, \beta_k) \tag{3.13}$$

Since $f(\alpha_k) = 0$, from (3.13) we have

$$f \text{ is strictly negative on the interval } (\alpha_k, \beta_k) \tag{3.14}$$

Combining (3.11) and (3.14) yields the desired contradiction.
We have proved the Lemma. □

Lemma 3.5. If $\mathcal{C}(f) = \mathcal{V}(f)$, then $a^*(f) = x^*(f)$.

Proof. Suppose that

$$\mathcal{V}(f) = \mathcal{C}(f)$$

From Lemma 3.3, we have

$$\mathcal{V}(f^{(i)}) = \mathcal{C}(f^{(i)}), \quad i = 1, \ldots, d$$

Hence we can repeatedly apply Lemma 3.4 to show that

$$x^*(f^{(r)}) \leq \cdots \leq x^*(f^{(1)}) \leq x^*(f)$$

where r is the largest index such that $f^{(r)}$ has a positive root. Hence

$$x^*(f) = a^*(f)$$

We have proved the Lemma. □

Proof of Theorem 3.2. From Theorem 2.3 of [22], we have

$$\frac{B_H(f)}{a^*(f)} \leq \frac{2d}{\ln(2)} \qquad \text{if } \deg(f) = d \tag{3.15}$$

Hence

$$\begin{aligned}
\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=\mathcal{C}(f)}} R_{B_H}(f) &= \sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=\mathcal{C}(f)}} \frac{B_H(f)}{x^*(f)} \\
&= \sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=\mathcal{C}(f)}} \frac{B_H(f)}{a^*(f)} && \text{from Lemma 3.5} \\
&\leq \sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=\mathcal{C}(f)}} \frac{2d}{\ln(2)} && \text{from (3.15)} \\
&= \frac{2d}{\ln(2)}
\end{aligned}$$

We have proved Theorem 3.2. □

3.4 Proof of Theorem "Over-Estimation when there is a single sign variation"

In this section, we will prove Theorem 3.3. Let f be a polynomial with positive leading coefficient and $\mathcal{V}(f) = 1$. Note that $a_d > 0$ and $a_t < 0$, where a_t is the trailing coefficient of f. We will crucially exploit the following polynomial

$$g \;=\; -x^d f\left(\frac{1}{x}\right).$$

We begin by claiming and proving a key lemma.

Lemma 3.6. $\frac{1}{B_H(g)} \geq \frac{1}{4} B_H(f)$.

Proof. Repeatedly rewriting g, we have

$$g = -x^d f\left(\frac{1}{x}\right) = -x^d \sum_{i=0}^{d} a_i x^{-i} = \sum_{i=0}^{d} -a_i x^{d-i} = \sum_{j=0}^{d} -a_{d-j} x^j = \sum_{j=0}^{d} b_j x^j$$

where $b_j = -a_{d-j}$. Note that g has a positive leading coefficient (namely, $-a_t$) and at least one negative coefficient. Recalling the definition of B_H, we have

$$B_H(g) = 2 \max_{\substack{q \\ b_q<0}} \min_{\substack{p \\ b_p>0 \\ p>q}} \left|\frac{b_q}{b_p}\right|^{\frac{1}{p-q}} = 2 \max_{\substack{q \\ -a_{d-q}<0}} \min_{\substack{p \\ -a_{d-p}>0 \\ p>q}} \left|\frac{-a_{d-q}}{-a_{d-p}}\right|^{\frac{1}{p-q}} = 2 \max_{\substack{q \\ a_{d-q}>0}} \min_{\substack{p \\ a_{d-p}<0 \\ p>q}} \left|\frac{a_{d-q}}{a_{d-p}}\right|^{\frac{1}{p-q}}$$

For later convenience, we carry out the somewhat unusual re-indexing $d-q \to p$ and $d-p \to q$, obtaining

$$B_H(g) = 2 \max_{\substack{p \\ a_p>0}} \min_{\substack{q \\ a_q<0 \\ d-q>d-p}} \left|\frac{a_p}{a_q}\right|^{\frac{1}{(d-q)-(d-p)}} = 2 \max_{\substack{p \\ a_p>0}} \min_{\substack{q \\ a_q<0 \\ p>q}} \left|\frac{a_p}{a_q}\right|^{\frac{1}{p-q}}$$

Since $\mathcal{V}(f) = 1$ and f has positive leading coefficient, the condition $p > q$ is redundant. Dropping the condition, we have

$$B_H(g) = 2 \max_{\substack{p \\ a_p>0}} \min_{\substack{q \\ a_q<0}} \left|\frac{a_p}{a_q}\right|^{\frac{1}{p-q}} \tag{3.16}$$

Note that the reciprocal of the maximum of a set of positive numbers is the minimum of the set of the reciprocals. Likewise, the reciprocal of the minimum is the maximum of the reciprocals. Thus we have

$$\frac{1}{B_H(g)} = \frac{1}{2} \min_{\substack{p \\ a_p>0}} \max_{\substack{q \\ a_q<0}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}}$$

Using the well known min-max inequality, we have

$$\frac{1}{B_H(g)} \geq \frac{1}{2} \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}}$$

By adding back the redundant the condition $p > q$, we have

$$\frac{1}{B_H(g)} \geq \frac{1}{2} \max_{\substack{q \\ a_q<0}} \min_{\substack{p \\ a_p>0 \\ p>q}} \left|\frac{a_q}{a_p}\right|^{\frac{1}{p-q}} \tag{3.17}$$

By combining the (3.17) and the definition of $B_H(f)$, we finally have

$$\frac{1}{B_H(g)} \geq \frac{1}{4} B_H(f).$$

We have proved the lemma. □

Proof of Theorem 3.3. We will first show that $\mathcal{R}_{B_H}(f) \leq 4$, using the previous Lemma. Note that the polynomial g has a positive leading coefficient, namely $-a_t$. It also has single sign variation. Thus from [22], we have

$$\mathcal{R}_{B_H}(g) \geq 1 \tag{3.18}$$

From Descartes' rule of sign, $x^*(f)$ is the unique positive root of f. Likewise $x^*(g)$ is the unique positive root of g. Thus, we have

$$\frac{1}{x^*(g)} = x^*(f) \tag{3.19}$$

By combining Lemma 3.6 and Equations (3.19) and (3.18), we have

$$\mathcal{R}_{B_H}(f) \;=\; \frac{B_H(f)}{x^*(f)} \;\leq\; \frac{4/B_H(g)}{1/x^*(g)} \;=\; 4\,\frac{x^*(g)}{B_H(g)} \;=\; 4/\mathcal{R}(g) \;\leq\; 4.$$

We will now show that the over-estimation bound is optimal. More precisely, we will show that there exist polynomials with positive leading coefficient, $\mathcal{V}(f) = 1$, and relative over-estimation arbitrarily close to 4. We will use the following family of polynomials paramterized by d as a "witness" for optimality.

$$h_d(x) = x^d + x^{d-1} + \cdots + x - 1.$$

Note that h_d has a positive leading coefficient and $\mathcal{V}(h_d) = 1$. Since every coefficient of h_d is ± 1, we have

$$B_H(h_d) \;=\; 2 \tag{3.20}$$

It is easy to verify that

$$\lim_{d\to\infty} x^*(h_d) = 1/2 \tag{3.21}$$

(In Appendix 3.A we include a detailed proof). Combining (3.20) and (3.21), we have

$$\lim_{d\to\infty} \mathcal{R}(h_d) = \frac{2}{1/2} = 4$$

We have proved Theorem 3.3. □

3.A Root of witness polynomials approaches 1/2

In this appendix, we prove equation 3.21. We require the following Lemma.

Lemma 3.7. For all $d > 0$, we have $x^*(h_d) > x^*(h_{d+1})$.

Proof. We will prove it by contradiction. Suppose that for some $d > 0$, we have

$$x^*(h_d) \leq x^*(h_{d+1}).$$

Then

$$x^*(h_d)^{d+1} + x^*(h_d)^d + \cdots + x^*(h_d) - 1 \leq x^*(h_{d+1})^{d+1} + x^*(h_{d+1})^d + \cdots + x^*(h_{d+1}) - 1 \quad (3.22)$$

From the definition of x^*, we have

$$x^*(h_d)^d + \cdots + x^*(h_d) - 1 = 0 \quad (3.23)$$

$$x^*(h_{d+1})^{d+1} + x^*(h_{d+1})^d + \cdots + x^*(h_{d+1}) - 1 = 0 \quad (3.24)$$

Combining (3.22), (3.23), and (3.24) we have

$$x^*(h_d)^{d+1} \leq 0$$

which contradict the fact that $x^*(h_d) > 0$. □

Proof of Equation 3.21. We will prove the limit using the squeeze theorem. First, we prove that the limit is bounded below by $\frac{1}{2}$. Let $d \geq 1$. Note that h_d has positive leading coefficient a single sign change. Hence from Theorem 3.3, we have

$$\mathcal{R}_{B_H}(h_d) \leq 4 \quad (3.25)$$

Since every coefficient of h_d is ± 1, we have

$$\mathcal{R}_{B_H}(h_d) = \frac{B_H(h_d)}{x^*(h_d)} = \frac{2 \cdot 1}{x^*(h_d)} \quad (3.26)$$

Plugging (3.26) into (3.25) and solving for $x^*(h_d)$ yields

$$x^*(h_d) \geq \frac{1}{2}$$

Hence

$$\lim_{d \to \infty} x^*(h_d) \geq \frac{1}{2} \quad (3.27)$$

We will now show that the limit is bounded above by $\frac{1}{2}$. Let $d \geq 2$. By definition, we have

$$h_d(\ x^*(h_d)\ ) \quad = \quad x^*(h_d)^d + \cdots + x^*(h_d) - 1 \quad = \quad 0 \tag{3.28}$$

We will perform the following rewrite:

$$x^*(h_d)^d + \cdots + x^*(h_d) - 1 \quad = \quad x^*(h_d)^d + \cdots + x^*(h_d) + 1 - 2 \tag{3.29}$$

By combining (3.28) and (3.29), we have

$$x^*(h_d)^d + \cdots + x^*(h_d) + 1 = 2$$

Since

$$x^*(h_d)^d + \cdots + x^*(h_d) + 1 = \frac{1 - x^*(h_d)^{d+1}}{1 - x^*(h_d)}$$

we have

$$\frac{1 - x^*(h_d)^{d+1}}{1 - x^*(h_d)} = 2$$

We will now solve for $x^*(h_d)$.

$$\begin{aligned} \frac{1 - x^*(h_d)^{d+1}}{1 - x^*(h_d)} &= 2 \\ 1 - x^*(h_d)^{d+1} &= 2 - 2x^*(h_d) \\ 2x^*(h_d) &= 1 + x^*(h_d)^{d+1} \\ x^*(h_d) &= \frac{1}{2} + \frac{x^*(h_d)^{d+1}}{2} \end{aligned}$$

Note that by Lemma 3.7, we have

$$x^*(h_d) \quad \leq \quad x^*(h_2) \quad < \quad x^*(h_1) \quad = \quad 1$$

Hence

$$x^*(h_d) \leq \frac{1}{2} + \frac{x^*(h_2)^{d+1}}{2}$$

where $x^*(h_2) < 1$. It follows that

$$\lim_{d \to \infty} x^*(h_d) \leq \lim_{d \to \infty} \frac{1}{2} + \frac{x^*(h_2)^{d+1}}{2} = \frac{1}{2} \tag{3.30}$$

By combining (3.27) and (3.30) and applying the squeeze theorem, we have

$$\lim_{d\to\infty} x^*(h_d) = \frac{1}{2}$$

□

3.B Average relative over-estimation for polynomials with single sign variation

In this appendix, we observe that the average value of $\mathcal{R}_{B_H}(f)$ is affected by the index of the first negative coefficient of f. To generate data points, we found the average value of $\mathcal{R}_{B_H}(f)$

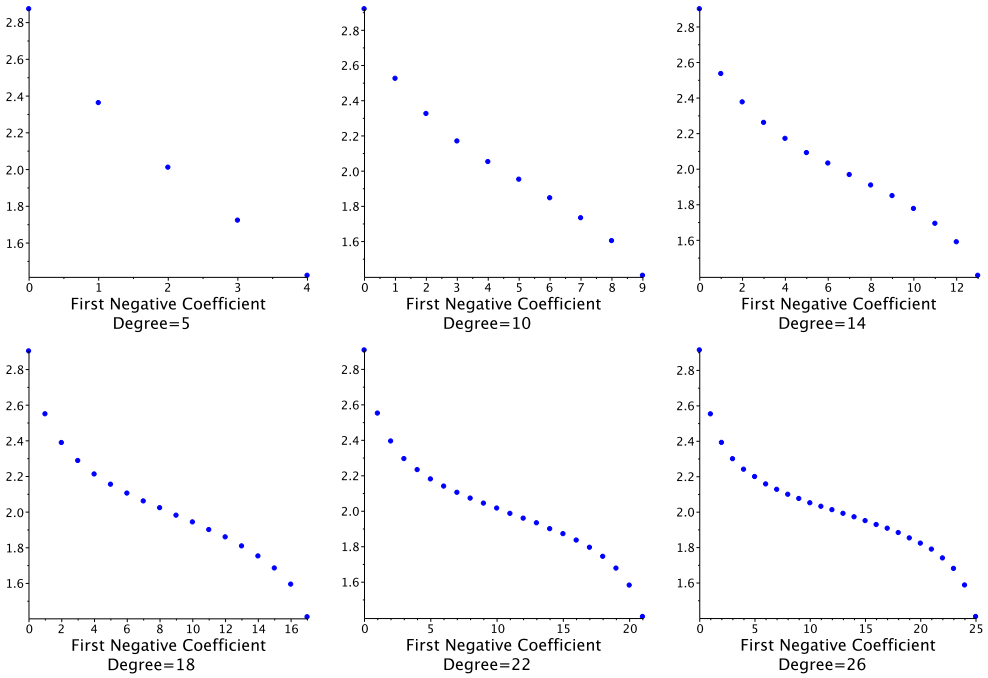

Figure 3.2: Average value of $\mathcal{R}_{B_H}(f)$ for fixed sign change location

for 1000 randomly generated polynomials of the form

$$a_d x^d + \cdots + a_{k+1}x^{k+1} - a_k x^k - \cdots - a_0$$

where k is the index of the first negative coefficient, $a_d, a_k \neq 0$, $a_i \in \mathbb{Z}_{\geq 0}$, and $0 \leq a_i \leq 1000$. All experiments were performed in Maple. It is clear from the plots that the average overestimation decreases as the sign change location increases.

Note that the above plots demonstrate the *average* behavior of $\mathcal{R}_{B_H}(f)$. A natural question is whether we can improve the overestimation bound using the index of the first negative coefficient. The set of polynomials

$$g_{d,k} = x^d + \cdots + x^{k+1} - x^k$$

can be used to show that we cannot significantly improve the constant in Theorem 3.3. For fixed d, $\mathcal{R}_{B_H}(f)$ rapidly approaches 4 as k decreases. We illustrate this behavior by plotting $\mathcal{R}_{B_H}(g_{26,k})$ for $k = 0, \ldots, 25$ in Figure 3.3.

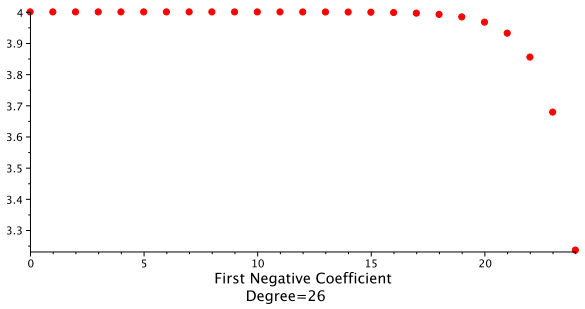

Figure 3.3: $\mathcal{R}_{B_H}(g_{26,k})$ for $k = 0, \ldots, 25$

3.C Relative over-estimation when the number of sign variations is not equal to the number of positive roots

We have already shown that relative over-estimation bounds can be derived when the number of sign variations is equal to the number of positive roots. We have also shown that when the sign variation is fixed at 1, a *tight* over-estimation bound exists for B_H. A natural question to ask is if we can derive a relative over-estimation bound which depends on the number of sign variations, even when the number of sign variations is not equal to the number of positive roots. It turns out that the answer to this question is no. In this appendix, we precisely prove this statement.

Proposition 3.1. Let $B : \mathbb{R}[x] \to \mathbb{R}_+$ be an absolute positivity bound. Let $k \geq 3$ and $d \geq k$.

Then

$$\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=k \\ 0<\mathcal{C}(f)<\mathcal{V}(f)}} \mathcal{R}_B(f) = \infty$$

Remark 3.4. By Descartes Rule of Signs, if $\mathcal{V}(f) = 2$, then f has 0 or 2 positive roots. Hence if $\mathcal{V}(f) = 2$,

$$0 < \mathcal{C}(f) < \mathcal{V}(f)$$

is impossible.

Proof of Proposition 3.1. We will distinguish between two cases: k odd and k even.

Suppose that k is odd. Define the following set of polynomials:

$$U = \{f_c : 0 < c \leq \frac{1}{3}\}$$

where

$$\begin{aligned} f_c(x) &= g_c(x) + \frac{c}{2} \\ g_c(x) &= (x+1)^{d-k}(x-c)(x-1)^{k-1} \end{aligned}$$

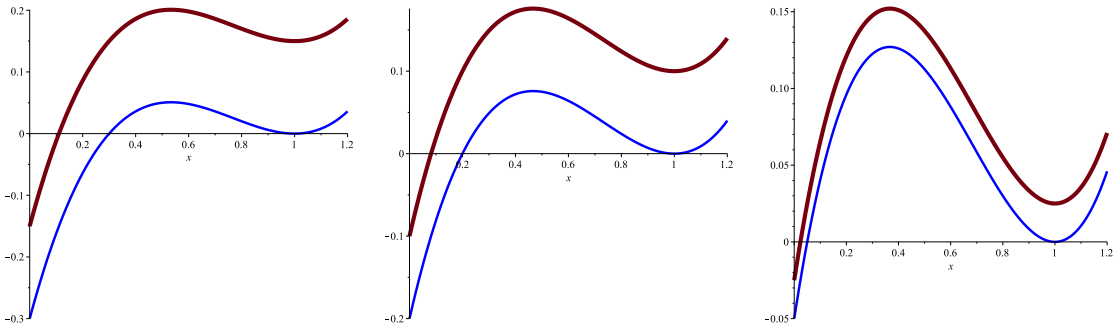

Figure 3.4: Plot of f_c (red) and g_c (blue) for $d = k = 3$ and $c = .3$ (left), $c = .2$ (middle), $c = .05$ (right).

We will first show that

$$U \subset \{f : f \text{ satisfies Assumption 3.1}, \ \deg(f) = d, \ \mathcal{V}(f) = k, \ 0 < \mathcal{C}(f) < \mathcal{V}(f)\}$$

Clearly, $\deg(f_c) = d$ for all c. By construction, f_c has positive leading coefficient and a single positive root, which is in the interval $(0, c)$. We will now show that $\mathcal{V}(f_c) = k$. Note that g_c is a polynomial with all real roots and exactly k positive roots. Hence by Descartes rule of signs, $v(g_c) = k$. Since the trailing coefficient of f_c is

$$-c + \frac{c}{2} = -\frac{c}{2} < 0$$

and every higher degree coefficient of f_c is unchanged from g_c, it follows that $\mathcal{V}(f_c) = k$. Since f_c has a single positive root and $k \geq 3$, we have

$$0 < \mathcal{C}(f) < k = \mathcal{V}(f)$$

Hence

$$U \subset \{f : f \text{ satisfies Assumption 3.1}, \ \deg(f) = d, \ \mathcal{V}(f) = k, \ 0 < \mathcal{C}(f) < \mathcal{V}(f)\} \tag{3.31}$$

We will now show that for all $0 < c \leq \frac{1}{3}$

$$x^*(f_c) \leq c \ \text{ and } \ B(f_c) \geq 1$$

Since $k \geq 3$, $k-1 \geq 2$. Hence $x = 1$ is a multiple root of g_c, and so $g'(1) = 0$. Since $f_c'(x) = g_c'(x)$, we have $f_c'(1) = 0$. Since B is an absolute positivity bound, we have

$$B(f_c) \geq 1 \tag{3.32}$$

Since the leading coefficient of g is positive and 1 is the largest positive root of g_c, g_c is strictly positive on the interval $(1, \infty)$. Since k is odd, $k - 1$ is even. Hence g_c is also strictly positive on the interval $(c, 1)$. Hence

$$f_c = g_c + \frac{c}{2}$$

is strictly positive on the interval (c, ∞). Hence, f_c has no roots which are larger than c. Thus

$$x^*(f_c) \leq c \tag{3.33}$$

To complete the proof of the claim for the case when k is odd, note that

$$\begin{aligned} \lim_{c \to 0} \mathcal{R}_B(f_c) &= \lim_{c \to 0} \frac{B(f_c)}{x^*(f_c)} \\ &\geq \lim_{c \to 0} \frac{1}{x^*(f_c)} \qquad \text{from (3.32)} \end{aligned}$$

$$\geq \lim_{c \to 0} \frac{1}{c} \qquad \text{from (3.33)}$$
$$= \infty \tag{3.34}$$

Combining (3.31) and (3.34), we have

$$\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=k \\ 0<\mathcal{C}(f)<\mathcal{V}(f)}} \mathcal{R}_B(f) = \infty \quad \forall \text{ odd } k \geq 3 \tag{3.35}$$

We now consider the case when k is even. We will use a similar strategy to the above. Define the following set of polynomials:

$$U = \{f_c : 0 < c \leq \frac{1}{3}\}$$

where

$$\begin{aligned} f_c(x) &= g_c + \epsilon(c) \\ g_c(x) &= (x+1)^{d-k}(x-c)(x-2c)(x-1)^{k-2} \\ \epsilon(c) &= \text{any positive number} < \max_{c<x<2c} |g_c(x)| \end{aligned}$$

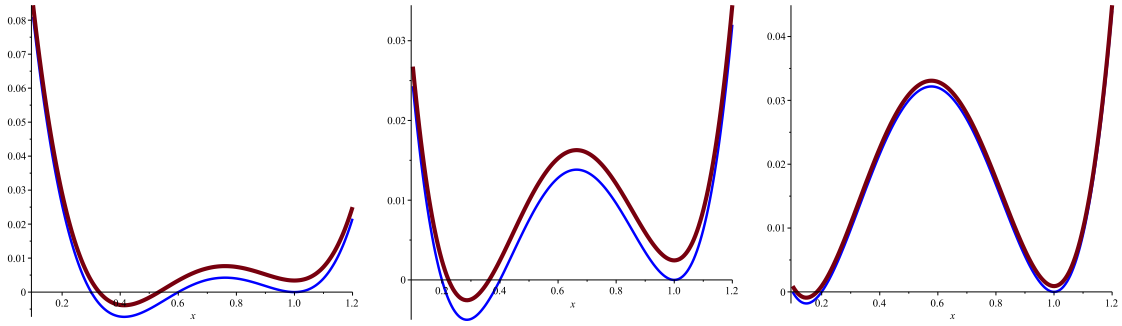

Figure 3.5: Plot of f_c (red) and g_c (blue) with appropriately chosen $\epsilon(c)$ for $d = k = 4$ and $c = .3$ (left), $c = .2$ (middle), $c = .1$ (right).

We will first show that

$$U \subset \{f : f \text{ satisfies Assumption 3.1}, \ \deg(f) = d, \ \mathcal{V}(f) = k, \ 0 < \mathcal{C}(f) < \mathcal{V}(f)\}$$

Clearly, $\deg(f_c) = d$ for all c. By construction, f_c has positive leading coefficient and 2 positive roots, which are in the interval $(c, 2c)$. It remains to be shown that $\mathcal{V}(f) = k$. Since the trailing coefficient of g is positive, $\epsilon(c) > 0$, and every higher degree coefficient of f_c is unchanged from g_c, it follows that $\mathcal{V}(f_c) = k$. Since f_c has 2 positive roots and $k \geq 4$, we have

$$0 < \mathcal{C}(f) < k = \mathcal{V}(f)$$

Hence

$$U \subset \{f : f \text{ satisfies Assumption 3.1}, \ \deg(f) = d, \ \mathcal{V}(f) = k, \ 0 < \mathcal{C}(f) < \mathcal{V}(f)\} \tag{3.36}$$

We will now show that for all $0 < c \leq \frac{1}{3}$

$$x^*(f_c) \leq 2c \ \text{ and } \ B(f) \geq 1$$

Since $k \geq 4$, $k-2 \geq 2$. Hence $x = 1$ is a multiple root of g_c, and so $g'(1) = 0$. Since $f_c'(x) = g_c'(x)$, we have $f_c'(1) = 0$. Since B is an absolute positivity bound, we have

$$B(f_c) \geq 1 \tag{3.37}$$

Since the leading coefficient of g is positive and 1 is the largest positive root of g_c, g_c is strictly positive on the interval $(1, \infty)$. Since k is odd, $k - 1$ is even. Hence g_c is also strictly positive on the interval $(2c, 1)$. Hence

$$f_c = g_c + \epsilon(c)$$

is strictly positive on the interval $(2c, \infty)$. Hence, f_c has no roots which are larger than c. Thus

$$x^*(f_c) \leq 2c \tag{3.38}$$

To complete the proof of the claim for the case when k is even, note that

$$\begin{aligned}
\lim_{c \to 0} \mathcal{R}_B(f_c) &= \lim_{c \to 0} \frac{B(f_c)}{x^*(f_c)} \\
&\geq \lim_{c \to 0} \frac{1}{x^*(f_c)} && \text{from (3.37)} \\
&\geq \lim_{c \to 0} \frac{1}{c} && \text{from (3.38)} \\
&= \infty && (3.39)
\end{aligned}$$

Combining (3.36) and (3.39), we have

$$\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=k \\ 0<\mathcal{C}(f)<\mathcal{V}(f)}} \mathcal{R}_B(f) = \infty \quad \forall \text{ even } k \geq 4 \tag{3.40}$$

Finally, combining (3.35) and (3.40), we have

$$\sup_{\substack{\deg(f)=d \\ \mathcal{V}(f)=k \\ 0<\mathcal{C}(f)<\mathcal{V}(f)}} \mathcal{R}_B(f) = \infty$$

We have proved Proposition 3.1.

□

Chapter 4

Root Separation Bounds of Univariate Polynomials

Introduction

In this chapter we present a new improved root separation bound for univariate polynomials. Root separation bounds are fundamental tools in algorithmic mathematics, with numerous applications [21, 31, 19, 8, 46, 52, 55, 9, 51]. As a consequence, there has been intensive effort in finding and studying such bounds [33, 37, 43, 40, 52, 18, 11, 12, 7, 45], resulting in many important bounds. Unfortunately, it is well known that current bounds are very pessimistic. Furthermore, we have found another issue with current bounds. If the roots of a polynomial are doubled, the root separation is obviously doubled. Hence we naturally expect that a root separation bound would double if the roots are doubled. This does not happen: frequently, the well known Mahler-Mignotte becomes even *smaller* when the roots are doubled. In other words, root separations bounds do not scale correctly; they are not compatible with the geometry of the roots. (We elaborate further on this phenomena in the next section).

So we have a challenge. Namely, we want to find new root separation bounds such that

1. the new bounds are less pessimistic (or almost always less pessimistic) than known bounds
2. the new bounds scale correctly
3. and of course, the new bounds can be computed efficiently.

The main contribution of this chapter is to provide a new univariate root separation bound which meets the challenge. We derive the new bound by transforming the celebrated Mahler-Mignotte Bound [33, 37] into a new bound which meets the challenge. Experimental evidence

indicates that the improvement is usually very large, especially when the magnitude of roots are different from 1.

The structure of this chapter is as follows. In Section 4.1 we elaborate on the challenge discussed above. In Section 4.2 we present the new univariate bound which meets the challenge. In Section 4.3 we derive the new bound. In Section 4.4 we discuss the experimental performance of the new bound.

4.1 Challenge

In order to motivate our search for new root separation bounds, we recall the celebrated Mahler-Mignotte root separation bound [33, 37].

$$B_{MM}(f) \;\; = \frac{\sqrt{3|dis(f)|}}{d^{d/2+1} \;\; ||f||_2^{d-1}}$$

where $dis(f)$ is the discriminant of f and d is the degree of f. Let us apply the Mahler-Mignotte bound to an example.

Example 4.1. Let $f(x) = x^4 - 60x^3 + 1000x^2 - 8000x$. As we saw in Example 2.4, the root separation of f is $\sqrt{200}$ (≈ 14.14). How does the Mahler-Mignotte bound perform on this polynomial? Let's see. We have

$$|dis(f)| = 2.56 \times 10^{16}, \quad ||f||_2 = 8.06 \times 10^3$$

and obviously the degree of f is 4. Combining these pieces, we have

$$B_{MM}(\, f(x)\,) \;=\; 8.26 \times 10^{-6}.$$

This bound is *significantly* smaller than the root separation of f (by several orders of magnitude)!

Now we consider the polynomial $f(x/2)$. Obviously, the root separation of $f(x/2)$ is twice the root separation of f. Hence we naturally expect that the Mahler-Mignotte bound of $f(x/2)$ is twice the Mahler-Mignotte bound of f. Let's see what happens.

$$B_{MM}(\, f(x/2)\,) \;=\; 1.05 \times 10^{-6}$$

It is not twice the Mahler-Mignotte bound of f. In fact, it is even *smaller* than the Mahler-Mignotte bound of f! This is very surprising. Maybe this is a peculiarity of our choice of 2. We

will try scaling by a different number.

$$B_{MM}(\, f(x/3)\,) \;=\; 3.12 \times 10^{-7}$$

What happened? The Mahler-Mignotte bound of $f(x/3)$ is *even smaller* than the Mahler-Mignotte bound of $f(x/2)$. It appears that the Mahler-Mignotte bound is *decreasing* as we *increase* the distance between the roots. Can this be true? Lets calculate $B_{MM}(\, f(x/s)\,)$ for many different values of s and see. In Figure 4.1 we plot $B_{MM}(\, f(x/s)\,)$.

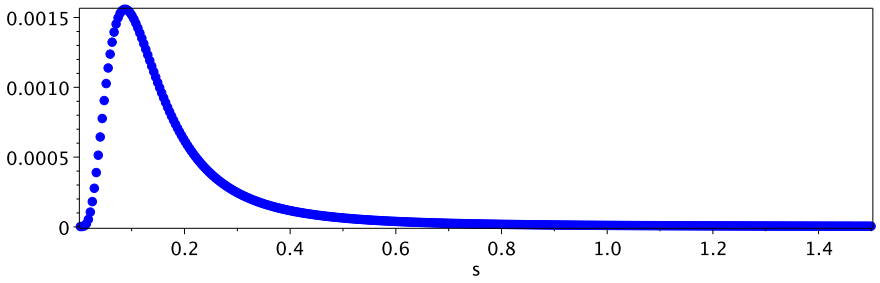

Figure 4.1: $B_{MM}(\, f(x/s)\,)$

Unfortunately, our suspicions are correct. Look at $s = 1$, where $B_{MM}(\, f(x/1)\,)$ is simply the Mahler-Mignotte bound of f. To the right of $s = 1$, the function $B_{MM}(\, f(x/s)\,)$ is decreasing. In fact, the Mahler-Mignotte bound is approaching *zero* as the root separation increases. The situation is equally strange to the left of the Mahler-Mignotte bound of f. When we decrease s, we see that until s reaches a value around .18, the Mahler-Mignotte bound is increasing. In other words, the Mahler-Mignotte bound is *increasing* when the root separation is *decreasing*. This is very odd. □

Let us summarize the observations from the above example.

1. The Mahler-Mignotte bound is very pessimistic (several magnitudes smaller than the root separation).

2. The Mahler-Mignotte bound does not scale correctly ("covariantly") with the roots of f.

We have also observed similar phenomena for other efficiently computable root separation bounds. So, we have a challenge.

Challenge 4.1. Find a function $B : \mathbb{C}[x] \to \mathbb{R}_+$ such that

1. $B(f)$ is a root separation bound.

2. $B(f)$ is almost always larger (hence less pessimistic) than known root separation bounds.

3. $B(f)$ scales covariantly.

4. $B(f)$ can be computed efficiently.

The main contribution of this chapter is a new root separation bound which meets the challenge.

4.2 Main Result

In this section we will precisely state the main result of the chapter. We require the following notation.

Notation 4.1.

$$\begin{array}{lcl} f & = & \sum_{i=0}^{d} a_i x^i = a_d \prod_{i=1}^{d} (x - \alpha_i) \in \mathbb{C}[x] \\ \Delta(f) & = & \min |\alpha_i - \alpha_j| \\ dis(f) & = & a_d^{2d-2} \prod_{i \neq j} (\alpha_i - \alpha_j) \end{array}$$

Definition 4.1. A function $B : \mathbb{C}[x] \to \mathbb{R}_+$ is a *root separation bound* if $B(f) \leq \Delta(f)$ for all $f \in \mathbb{C}[x]$.

We begin by recalling the Mahler-Mignotte bound [33, 37]

$$B_{MM,k}(f) = \frac{\sqrt{|dis(f)|}}{||f||_k^{d-1}} P_k(d)$$

where

$$P_k(d) = \frac{\sqrt{3}}{d^{d/2+1}(d+1)^{(\frac{1}{2}-\frac{1}{k})(d-1)}}.$$

We are now ready to present the main contribution of this chapter: a new univariate root separation bound which meets the challenge in the previous section.

Definition 4.2 (New Univariate Bound)**.** Let $k \geq 2$. Define

$$B_{New,k}(f) = \frac{\sqrt{|dis(f)|}}{H_k^{d-1}} P_k(d)$$

where

$$H_k = \frac{\left\| \sum_{i=0}^{d} \tilde{s}_k^{d-i} a_i \cdot x^i \right\|_k}{\tilde{s}^{\frac{d}{2} - \frac{1}{d-1}}}$$

$$\tilde{s}_k = \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}}$$

$$h(i) = \frac{d}{2} - i + \frac{1}{d-1}$$

Theorem 4.1 (New Univariate Bound)**.** Let $k \geq 2$. Then

1. $B_{New,k}$ is a root separation bound.
2. If $k = \infty$, then $B_{New,k} \geq B_{MM,k}$ (when $k < \infty$, see the discussion in the following remark).
3. $B_{New,k}$ scales covariantly.
4. $\tilde{s}_k$ can be computed in $\mathcal{O}(d)$ algebraic operations and comparisons using Algorithm 4.

Example 4.2. Let $f = x^4 - 60x^3 + 1000x^2 - 8000x$. Recall that the root separation of f is approximately 14.14. We have

$$\begin{aligned}
B_{MM,\infty} &= 7.56 \times 10^{-7} \\
\tilde{s}_\infty &= \max_{q \in \{3,4\}} \min_{p \in \{1,2\}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}} \\
&= \max \left\{ \min \left\{ \left(\frac{|60|}{|8000|} \right)^{\frac{1}{3-1}}, \left(\frac{|60|}{|1000|} \right)^{\frac{1}{3-2}} \right\}, \min \left\{ \left(\frac{|1|}{|8000|} \right)^{\frac{1}{4-1}}, \left(\frac{|1|}{|1000|} \right)^{\frac{1}{4-2}} \right\} \right\} \\
&= \max \left\{ 6.00 \times 10^{-2}, 3.16 \times 10^{-2} \right\} \\
&= 6.00 \times 10^{-2} \\
H_\infty &= \frac{||x^4 - 3.60x^3 + 3.60x^2 - 1.73x||_\infty}{(6.00 \times 10^{-2})^{\frac{4}{2} - \frac{1}{4-1}}} \\
&= \frac{3.60}{(6.00 \times 10^{-2})^{\frac{5}{3}}} \\
&= 3.91 \times 10^2 \\
B_{New,\infty} &= 6.45 \times 10^{-3}
\end{aligned}$$

Note that $B_{New,\infty}$ is a root separation bound for f, and is significantly larger than $B_{MM,\infty}$. To demonstrate the covariance, we plot the function $B_{New,\infty}(\, f(x/s)\,)$ in Figure 4.2. □

Remark 4.1. Experimental evidence indicates that $B_{New,k}$ is almost always larger than $B_{MM,k}$ for finite k. For example, with the same polynomial as in the preceding examples, we have

$$B_{New,2}(f) \;=\; 2.02 \times 10^{-2} \;\gg\; B_{MM,2}(f) \;=\; 8.26 \times 10^{-6}$$

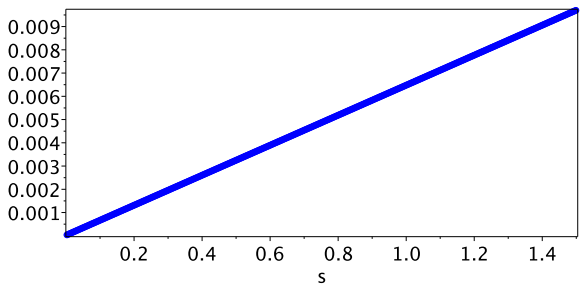

Figure 4.2: Scaling covariance of $B_{New,\infty}$

Furthermore, $B_{New,k}$ is almost always larger for *smaller* k, as the same example illustrates:

$$B_{New,2}(f) \;=\; 2.02 \times 10^{-2} \;\;>\;\; B_{New,\infty}(f) \;=\; 6.45 \times 10^{-3}$$

In Section 4.4 we will provide theoretical justification for this observation.

Remark 4.2. For square-free integer polynomials, the discriminant has a lower bound of 1. Hence in practice the discriminant is almost always replaced by 1. In this case, part (4) of Theorem 4.1 implies that $B_{New,k}$ can be computed in $\mathcal{O}(d)$ algebraic operations and comparisons. Note that removing the discriminant sacrifices the scaling covariance.

4.3 Derivation

4.3.1 Overall framework

In this subsection, we present the framework we will use to derive the new bound. We require the following notation.

Notation 4.2.

- $f^{(s)} = s^d f(\, x/s\,)$

Note that in the above notation we scale the roots of f using a slight modification of the scaling operation in the introduction. Since the only difference between the two scaling operation are the leading coefficients, the two operations are equivalent. We use this scaling operation for later convenience. In Propositions 4.1-4.3 we will incrementally develop the framework used to meet the challenge stated at the beginning of this chapter.

Proposition 4.1 (Scaled Bound)**.** Let $B : \mathbb{C}[x] \to \mathbb{R}_+$ be a root separation bound and $s \in \mathbb{R}_+$. Let

$$B^* : f \mapsto \frac{B(f^{(s)})}{s}$$

Then

1. B^* is a root separation bound.

We will illustrate the result by a simple example, since the proof is simple.

Example 4.3. Let $f(x) = x^4 - 60x^3 + 1000x^2 - 8000x$. We have

$$B_{MM,2}(\, f^{(2)}\,) \;=\; B_{MM,2}(\, 2^4 f(x/2)\,) \;=\; 1.05 \times 10^{-6}. \tag{4.1}$$

Since $B_{MM,2}$ is a root separation bound, it follows that

$$B_{MM,2}(\, f^{(2)}\,) \;\leq\; \Delta(\, f^{(2)}\,) \;=\; 2\,\Delta(f)$$

Rearranging yields

$$\frac{B_{MM,2}(\, f^{(2)}\,)}{2} \leq \Delta(f) \tag{4.2}$$

Combining (4.1) and (4.2) we have

$$\frac{1.05 \times 10^{-6}}{2} \;=\; 5.25 \times 10^{-7} \;\leq\; \Delta(f).$$

Note that $5.25 \times 10^{-7} \leq B_{MM,2}(f)$. So 2 was not a good choice for s.

How should we choose s? In Figure 4.3 we plot the function $B_{MM,2}(\, f^{(s)}\,)/s$. Clearly, we should choose s so that the function is maximized. We see that for $s \approx .16$, the the new bound is approximately 2.00×10^{-2}. This new bound is significantly larger than $B_{MM,2}(f) = 8.26 \times 10^{-6}$. □

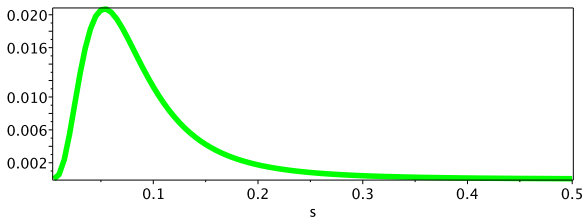

Figure 4.3: Scaled bound for $B_{MM,2}$ and f.

Proposition 4.2 (Covariant Bound)**.** Let $B : \mathbb{C}[x] \to \mathbb{R}_+$ be a root separation bound and $\sigma : \mathbb{C}[x] \to \mathbb{R}_+$. Let

$$B^* : f \mapsto \frac{B(f^{(\sigma(f))})}{\sigma(f)}$$

If $\forall f \in \mathbb{C}[x]$ and $\forall \gamma > 0$ we have

$$\sigma(f^{(\gamma)}) = \frac{1}{\gamma}\sigma(f)$$

then

1. B^* is a root separation bound.
2. B^* scales covariantly

Proof. The first property follows from Proposition 4.1.

We will now prove the second property. Let $f \in \mathbb{C}[x]$ and $\gamma > 0$. By definition

$$B^*(f^{(\gamma)}) \;=\; \frac{B\left(\left(f^{(\gamma)}\right)^{(\sigma(f^{(\gamma)}))}\right)}{\sigma(f^{(\gamma)})}$$

Since $\sigma(f^{(\gamma)}) = \frac{1}{\gamma}\sigma(f)$, we have

$$\left(f^{(\gamma)}\right)^{(\sigma(f^{(\gamma)}))} = f^{(\gamma\sigma(f^{(\gamma)})} = f^{(\gamma\cdot\frac{1}{\gamma}\cdot\sigma(f))} = f^{(\sigma(f))} \tag{4.3}$$

Hence

$$B^*(f^{(\gamma)}) = \frac{B\left(\left(f^{(\gamma)}\right)^{\sigma(f^{(\gamma)})}\right)}{\sigma(F^{(\gamma)})} = \frac{B(F^{(\sigma(f))})}{\sigma(F^{(\gamma)})} \qquad \text{from (4.3)}$$
$$= \frac{B(f^{(\sigma(f))})}{\frac{1}{\gamma}\sigma(f)} = \gamma\frac{B(f^{(\sigma(f))})}{\sigma(f)} = \gamma B^*(f)$$

We have proved that B^* scales covariantly. □

Proposition 4.3 (Optimal Bound)**.** Let $B : \mathbb{C}[x] \to \mathbb{R}_+$ be a root separation bound. Let

$$B^* : f \mapsto \max_s \frac{B(f^{(s)})}{s}$$

Then

1. B^* is a root separation bound.
2. B^* scales covariantly
3. $B^*(f) \geq B(f)$

Proof. The first property follows from Proposition 4.1.

To prove the second property, we will show that σ has the scaling property described in Proposition 4.2. Let $f \in \mathbb{C}[x]$ and $\gamma > 0$. We have

$$\begin{aligned}
\sigma(f^{(\gamma)}) &= \arg\max_{s>0} \frac{B\left(\left(f^{(\gamma)}\right)^{(s)}\right)}{s} \\
&= \arg\max_{s>0} \frac{B\left(f^{(\gamma s)}\right)}{s} \\
&= \arg\max_{s>0} \frac{1}{\gamma}\frac{B\left(f^{(\gamma s)}\right)}{s} && \text{since } \gamma > 0 \\
&= \arg\max_{s>0} \frac{B\left(f^{(\gamma s)}\right)}{s\gamma} \\
&= \frac{1}{\gamma}\arg\max_{s>0} \frac{B\left(f^{(s)}\right)}{s} \\
&= \frac{1}{\gamma}\sigma(f)
\end{aligned}$$

Hence by Proposition 4.2, B^* scales covariantly.

We will now prove the third property. We have

$$B^*(f) = \max_{s>0} \frac{B(\, f^{(s)}\,)}{s} \geq \frac{B(\, f^{(1)}\,)}{1} = \frac{B(f)}{1} = B(f)$$

We have proved the Proposition. □

Let us summarize the framework built up in this section. We have seen that

$$\max_{s>0} \frac{B(f^{(s)})}{s}$$

meets the challenge *if the maximum can be computed efficiently*. If the maximum cannot be computed efficiently, we can *approximate* the maximum. We can then use Proposition 4.2 to guarantee that the new bound is scaling covariant.

4.3.2 Derivation of New Univariate Bound

In this section we derive the new univariate bound. We will find a tight approximation $\tilde{s}_k$ of

$$s_k^* = \arg\max_{s>0} \frac{B_{MM,k}(\, f^{(s)}\,)}{s}$$

We will then use Proposition 4.2 and a result due to Melhorn and Ray to show that the bound

$$B_{New,k} = \frac{B_{MM,k}(\, f^{(\tilde{s}_k)}\,)}{\tilde{s}_k}$$

meets the challenge.

First, we find a find a simplified expression for s_k^*. We will take advantage of the following easily verifiable identities:

Lemma 4.1. Let $g : \mathbb{R}_+ \to \mathbb{R}_+$, and $c > 0$. Then

1. $\arg\max_{s>0}\ g(s) = \arg\max_{s>0}\ c \cdot g(s)$
2. $\arg\max_{s>0}\ g(s) = \arg\max_{s>0}\ (g(s))^c$
3. $(\arg\max_{s>0}\ g(s))^{-1} = \arg\min_{s>0} g(s)$

Lemma 4.2. Let $f \in \mathbb{C}[x]$. Then

$$s_k^* = \arg\min_{s>0} R_k(s)$$

where

$$R_k(s) = \frac{||f^{(s)}||_k}{s^{\frac{d}{2}-\frac{1}{d-1}}}$$

Proof. To prove the claim, we will expand the expression for

$$\frac{B_{MM,k}(\ f^{(s)}\ )}{s}$$

then simplify this expression with the identities of Lemma 4.1. We have

$$B_{MM,k}(\ f^{(s)}\ ) = \frac{\sqrt{|dis(f^{(s)})|}}{||f^{(s)}||_k^{d-1}} P_k(d) \tag{4.4}$$

Since

$$f^{(s)} = s^d\, f(x/s) = s^d\, a_d \prod_{i=1}^{d}(x/s - s\alpha_i) = a_d \prod_{i=1}^{d}(x - s\alpha_i)$$

we have

$$\begin{aligned} dis(f^{(s)}) &= a_d^{2d-2} \prod_{i\neq j}(s\alpha_i - s\alpha_j) \\ &= a_d^{2d-2} s^{d(d-1)} \prod_{i\neq j}(\alpha_i - \alpha_j) \\ &= s^{d(d-1)} dis(f) \end{aligned} \tag{4.5}$$

Hence

$$\begin{aligned} \frac{B_{MM,k}(f^{(s)})}{s} &= \frac{1}{s}\frac{\sqrt{|dis(f^{(s)})|}}{||f^{(s)}||_k^{d-1}} P_k(d) \\ &= \frac{1}{s}\frac{\sqrt{|s^{d(d-1)} dis(f)|}}{||f^{(s)}||_k^{d-1}} P_k(d) && \text{from (4.5)} \\ &= \frac{s^{\frac{d(d-1)}{2}}\sqrt{|dis(f)|}}{s||f^{(s)}||_k^{d-1}} P_k(d) \\ &= \frac{s^{\frac{d(d-1)}{2}-1}}{||f^{(s)}||_k^{d-1}} \sqrt{|dis(f)|} P_k(d) \\ &= \left(\frac{s^{\frac{d}{2}-\frac{1}{d-1}}}{||f^{(s)}||_k}\right)^{d-1} \sqrt{|dis(f)|} P_k(d) \\ &= \left(\frac{1}{R_k(s)}\right)^{d-1} \sqrt{|dis(f)|} P_k(d) \end{aligned} \tag{4.6}$$

Now we apply the identities from Lemma 4.1 to the expression in (4.6):

$$\begin{aligned}
\arg\max_{s>0} \frac{B_{MM,k}(\ f^{(s)}\ )}{s} &= \arg\max_{s>0} \left(\frac{1}{R_k(s)}\right)^{d-1} \sqrt{|dis(f)|} P_k(d) \\
&= \arg\max_{s>0} \left(\frac{1}{R_k(s)}\right)^{d-1} && \text{(Identity 1)} \\
&= \arg\max_{s>0} \left(\frac{1}{R_k(s)}\right) && \text{(Identity 2)} \\
&= \arg\min_{s>0} R_k(s) && \text{(Identity 3)}
\end{aligned}$$

We have proved the Lemma. □

Lemma 4.3. Let $k \geq 2$. Then

$$s_k^* = (t^*)^{\frac{1}{k}}$$

where t^* is the unique positive root of

$$Q_k(t) = \sum_{i=0}^{d} h(i) \left|a_i\right|^k \cdot t^{d-i}$$

and $h(i) = \frac{d}{2} - i + \frac{1}{d-1}$.

Proof. For later convenience, we first rewrite $R_k(s)$.

$$\begin{aligned}
R_k(s) &= \frac{||\ f^{(s)}\ ||_k}{s^{\frac{d}{2}-\frac{1}{d-1}}} \\
&= \frac{\left(\sum_{i=0}^{d} \left|s^{d-i} a_i\right|^k\right)^{\frac{1}{k}}}{s^{\frac{d}{2}-\frac{1}{d-1}}} \\
&= \frac{\left(\sum_{i=0}^{d} s^{kd-ki} \left|a_i\right|^k\right)^{\frac{1}{k}}}{s^{\frac{d}{2}-\frac{1}{d-1}}} \\
&= \left(\frac{\sum_{i=0}^{d} s^{kd-ki} \left|a_i\right|^k}{s^{\frac{kd}{2}-\frac{k}{d-1}}}\right)^{\frac{1}{k}} \\
&= \left(\sum_{i=0}^{d} s^{kd-ki-\left(\frac{kd}{2}-\frac{k}{d-1}\right)} \left|a_i\right|^k\right)^{\frac{1}{k}} \\
&= \left(\sum_{i=0}^{d} s^{\frac{kd}{2}-ki+\frac{k}{d-1}} \left|a_i\right|^k\right)^{\frac{1}{k}}
\end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{i=0}^{d} (s^k)^{\frac{d}{2} - i + \frac{1}{d-1}} |a_i|^k \right)^{\frac{1}{k}} \\
&= \left(\sum_{i=0}^{d} (s^k)^{h(i)} |a_i|^k \right)^{\frac{1}{k}} \qquad \text{since } h(i) = \frac{d}{2} - i + \frac{1}{d-1} \\
&= \tilde{R}_k(s)^{\frac{1}{k}} \qquad (4.7)
\end{aligned}
$$

Combining Lemma 4.1 and (4.7), we have

$$s_k^* = \arg\min_{s>0} R_k(s) = \arg\min_{s>0} \tilde{R}_k(s) \tag{4.8}$$

Hence from Calculus, we have

$$\tilde{R}_k'(s_k^*) = 0 \tag{4.9}$$

Note that

$$\tilde{R}_k'(s) = \sum_{i=0}^{d} s^{kh(i)-1} \cdot kh(i) |a_i|^k$$

Define the polynomial

$$Q_k(t) = \sum_{i=0}^{d} h(i) |a_i|^k \cdot t^{d-i}$$

We have

$$
\begin{aligned}
k s^{\frac{-kd}{2} - \frac{k}{d-1} - 1} Q_k(s^k) &= s^{-\frac{kd}{2} - \frac{k}{d-1} - 1} \sum_{i=0}^{d} kh(i) |a_i|^k \cdot (s^k)^{d-i} \\
&= s^{-\frac{kd}{2} - \frac{k}{d-1} - 1} \sum_{i=0}^{d} kh(i) |a_i|^k \cdot (s^k)^{d-i} \\
&= \sum_{i=0}^{d} s^{kd - ki - \frac{kd}{2} - \frac{k}{d-1} - 1} \cdot kh(i) |a_i|^k \\
&= \sum_{i=0}^{d} s^{\frac{kd}{2} - ki - \frac{k}{d-1} - 1} \cdot kh(i) |a_i|^k \\
&= \sum_{i=0}^{d} s^{\frac{kd}{2} - ki - \frac{k}{d-1} - 1} \cdot kh(i) |a_i|^k \\
&= \sum_{i=0}^{d} s^{k(\frac{d}{2} - i - \frac{1}{d-1}) - 1} \cdot kh(i) |a_i|^k
\end{aligned}
$$

$$= \sum_{i=0}^{d} s^{kh(i)-1} \cdot kh(i) \, |a_i|^k$$
$$= \tilde{R}'_k(s)$$

Hence

$$\tilde{R}'_k(s) = 0 \iff Q_k(s^k) = 0 \quad \forall s > 0 \tag{4.10}$$

Note that $Q_k(t)$ has a single sign change, since $h(i)$ is strictly decreasing with i. By Descartes Rule of Signs, $Q_k(t)$ has a single positive root t^*. Combining (4.8), (4.9), and (4.10), we have

$$s_k^* = (t^*)^{\frac{1}{k}}$$

We have proved the Lemma. □

Since Q_k is a polynomial with a single sign change, we can derive a tight approximation of its single positive root using Theorem 3.3.

Lemma 4.4. Let $f = \sum_{i=0}^{m} c_i x^{e_i}$ have a single sign change, and x^* be the unique positive root of f. Then

$$L \le x^* \le U$$

where

$$L = \frac{1}{2} \, \mathcal{H}(f)$$
$$U = 2 \, \mathcal{H}(f)$$
$$\mathcal{H}(f) = \max_{\substack{q \\ c_q<0}} \min_{\substack{p \\ c_p>0 \\ e_p>e_q}} \left(\frac{|c_q|}{|c_p|} \right)^{\frac{1}{e_p - e_q}}$$

Proof. The upper bound is simply the Hong bound applied to f. To derive the lower bound, solve for $x^*(f)$ in Theorem 3.3. □

Lemma 4.5. Let $k \ge 2$. Then

$$\left(\frac{1}{2} \right)^{\frac{1}{k}} (\mathcal{H}(Q_k))^{\frac{1}{k}} \le s_k^* \le 2^{\frac{1}{k}} \, (\mathcal{H}(Q_k))^{\frac{1}{k}}$$

Proof. From Lemma 4.3, we have

$$s_k^* = (t^*)^{\frac{1}{k}} \tag{4.11}$$

where t^* is the unique positive root of $Q_k(t)$. Since $Q_k(t)$ has single sign change, we can apply Lemma 4.4. We have

$$L \leq t^* \leq U \tag{4.12}$$

where

$$L = \frac{1}{2}\mathcal{H}(Q_k)$$
$$U = 2\mathcal{H}(Q_k)$$

Combining (4.11) and (4.12), we have

$$(L)^{\frac{1}{k}} \leq s_k^* \leq (U)^{\frac{1}{k}}$$

Equivalently

$$\left(\frac{1}{2}\right)^{\frac{1}{k}} (\mathcal{H}(Q_k))^{\frac{1}{k}} \leq s_k^* \leq 2^{\frac{1}{k}} (\mathcal{H}(Q_k))^{\frac{1}{k}}$$

We have proved the Lemma. □

Lemma 4.6. Let $k \geq 2$. We have

$$\tilde{s}_k = (\mathcal{H}(Q_k))^{\frac{1}{k}}$$

and

$$\lim_{k\to\infty} \tilde{s}_k = \mathcal{H}(G)$$

where

$$G = \sum_{\substack{p \\ h(p)>0}} \frac{1}{|a_p|} s^{d-p} - \sum_{\substack{q \\ h(q)<0}} \frac{1}{|a_q|} s^{d-q}$$

Proof. We have

$$\begin{aligned}
(\mathcal{H}(Q_k))^{\frac{1}{k}} &= \left(\max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\frac{|h(q)|\,|a_q|^k}{|h(p)|\,|a_p|^k} \right)^{\frac{1}{(d-p)-(d-q)}} \right)^{\frac{1}{k}} \\
&= \left(\max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\frac{|h(q)|\,|a_q|^k}{|h(p)|\,|a_p|^k} \right)^{\frac{1}{q-p}} \right)^{\frac{1}{k}} \\
&= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\frac{|h(q)|\,|a_q|^k}{|h(p)|\,|a_p|^k} \right)^{\frac{1}{k(q-p)}}
\end{aligned}$$

$$= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}}$$
$$= \tilde{s}_k$$

We now consider the limit. We have

$$\lim_{k\to\infty} \tilde{s}_k = \lim_{k\to\infty} \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}}$$
$$= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}}$$

We also have

$$\begin{aligned}
\mathcal{H}(G) &= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0 \\ (d-p)>(d-q)}} \left(\frac{\frac{1}{|a_q|}}{\frac{1}{|a_p|}} \right)^{\frac{1}{(d-p)-(d-q)}} \\
&= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0 \\ (d-p)>(d-q)}} \left(\frac{\frac{1}{|a_q|}}{\frac{1}{|a_p|}} \right)^{\frac{1}{q-p}} \\
&= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0 \\ (d-p)>(d-q)}} \left(\frac{|a_p|}{|a_q|} \right)^{\frac{1}{q-p}} \\
&= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0 \\ q<p}} \left(\frac{|a_p|}{|a_q|} \right)^{\frac{1}{q-p}} \\
&= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\frac{|a_p|}{|a_q|} \right)^{\frac{1}{q-p}} && \text{since } h(i) \text{ is strictly decreasing with } i \\
&= \lim_{k\to\infty} \tilde{s}_k
\end{aligned}$$

□

Lemma 4.7. Let $k \geq 2$ and

$$s_k^* = \arg\max_{s>0} \frac{B_{MM,k}(\, f^{(s)}\,)}{s}$$

Then

$$\left(\frac{1}{2}\right)^{\frac{1}{k}} \tilde{s}_k \;\leq\; s_k^* \;\leq\; 2^{\frac{1}{k}} \tilde{s}_k$$

where

$$\tilde{s}_k = \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}}$$

$$h(i) = \frac{d}{2} - i + \frac{1}{d-1}$$

Proof. Let $k \geq 2$ and

$$s_k^* = \arg\max_{s>0} \frac{B_{MM,k}(\, f^{(s)}\,)}{s}$$

Combining Lemmas 4.2, 4.5 and 4.6, we have

$$\left(\frac{1}{2}\right)^{\frac{1}{k}} \tilde{s}_k \;\leq\; s_k^* \;\leq\; 2^{\frac{1}{k}} \tilde{s}_k$$

We have proved the Lemma. □

We are now ready to define the new bound. From Lemma 4.7, we observe that $\tilde{s}_k$ is a tight approximation of s_k^*. As k increases, the approximation becomes tighter. Thus we choose to approximate the bound

$$\max_{s>0} \frac{B_{MM,k}(\, f^{(s}\,)}{s}$$

with the bound

$$B_{New,k}(f) \;=\; \frac{B_{MM,k}(\, f^{(\tilde{s}_k)}\,)}{\tilde{s}_k} \;=\; \frac{\sqrt{|dis(f)|}}{H_k^{d-1}} P_k(d) \tag{4.13}$$

Before proving Theorem 4.1, we present an algorithm for computing $\tilde{s}_k$. We combine Lemma 4.6 and the algorithm due to Melhorn and Ray (see [36] and Chapter 2) to compute $\mathcal{H}(Q)$ in $\mathcal{O}(d)$ algebraic operations and comparisons. We recall their complexity results in the Lemma below.

Lemma 4.8 (Melhorn, Ray, 2010 [36])**.** Let $g \in \mathbb{R}[x]$ with m non-zero coefficients. Then $\mathcal{H}(g)$ can be computed in $\mathcal{O}(m)$ algebraic operations and comparisons with the algorithm *Compute*$\mathcal{H}$ (Algorithm 3 in Chapter 2).

Proof of Theorem 4.1. We prove them one by one.

1. Combine (4.13) and Proposition 4.1.

Algorithm 4: *Compute$\tilde{s}$*

Input : $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{C}[x]$
$k \geq 2$

Output: $\tilde{s}_k$

```
begin
    if k is finite then
        Q ← Σ_{i=0}^{d} h(i) |a_i|^k · t^{d−i};
        s̃ ← ComputeH(Q)^{1/k}
    else
        Q ← Σ_{p, h(p)>0} (1/|a_p|) s^{d−p} − Σ_{q, h(q)<0} (1/|a_q|) s^{d−q};
        s̃ ← ComputeH(Q)
end
```

2. From Lemma 4.7, we have

$$\tilde{s}_\infty = s^*_\infty$$

Hence

$$\begin{aligned} B_{New,\infty}(f) &= \frac{B_{MM,\infty}(\ f^{(\tilde{s}_\infty)}\ )}{\tilde{s}_\infty} \\ &= \frac{B_{MM,\infty}(\ f^{(s^*_\infty)}\ )}{s^*_\infty} \\ &= \arg\max_{s>0} \frac{B_{MM,\infty}(\ f^{(s)}\ )}{s} \end{aligned}$$

Hence by Proposition 4.3, $B_{New,\infty}(f) \geq B_{MM,\infty}(f)$ for all f.

3. Let $\gamma > 0$. We have

$$\begin{aligned} \tilde{s}_k(f^{(\gamma)}) &= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{\gamma^{d-q}\,|a_q|}{\gamma^{d-p}\,|a_p|} \right)^{\frac{1}{(q-p)}} \\ &= \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \frac{1}{\gamma^{q-p}} \right)^{\frac{1}{(q-p)}} \\ &= \frac{1}{\gamma} \max_{\substack{q \\ h(q)<0}} \min_{\substack{p \\ h(p)>0}} \left(\left(\frac{|h(q)|}{|h(p)|} \right)^{\frac{1}{k}} \frac{|a_q|}{|a_p|} \right)^{\frac{1}{(q-p)}} \\ &= \frac{1}{\gamma} \tilde{s}_k \end{aligned}$$

Hence by Proposition 4.2, $B_{New,k}$ scales covariantly.

4. Combine Lemma 4.6, Lemma 4.8, and Algorithm 4.

We have completed the proof of Theorem 4.1. □

4.4 Performance

In this Section, we discuss the experimental performance of the new bound. We first repeat the observation of Remark 4.1: experimental evidence indicates that $B_{New,k}$ is almost always *larger* for *smaller* k. This is unsurprising once we consider the derivation strategy in the previous section. Let $k_1 \leq k_2$. We have

$$B_{New,k_1} \approx \max_{s>0} \frac{B_{MM,k_1}\left(\, f^{(s)} \,\right)}{s}, \qquad B_{New,k_2} \approx \max_{s>0} \frac{B_{MM,k_1}\left(\, f^{(s)} \,\right)}{s}$$

and

$$\max_{s>0} \frac{B_{MM,k_1}\left(\, f^{(s)} \,\right)}{s} \;\geq\; \frac{B_{MM,k_1}\left(\, f^{(s^*_{k_2})} \,\right)}{s^*_{k_2}} \;\geq\; \frac{B_{MM,k_2}\left(\, f^{(s^*_{k_2})} \,\right)}{s^*_{k_2}} \;=\; \max_{s>0} \frac{B_{MM,k_2}\left(\, f^{(s)} \,\right)}{s}$$

We have also observed that the improvement is usually very large for the new bounds, especially when the magnitude of roots are different from 1. To generate data points, we generated 100 random monic polynomials with fixed degree and height (defined below) and calculated the average value of the improvement:

$$\frac{B_{New,k}(f)}{B_{MM,k}(f)} = \left(\frac{||f_k||}{H_k}\right)^{d-1}$$

Note that the improvement is independent of the discriminant for both new bounds. This observation allowed us to avoid many expensive computations when performing experiments.

We defined the height of a monic polynomial with the binomial height:

$$||f||_B = \max_{0\leq i\leq d-1} \frac{|a_i|^{\frac{1}{d-i}}}{\binom{d}{i}}$$

It is well known that the binomial height is related to the size of the roots. To generate a polynomial with the height r_n/r_d, we uniformly generated an integer c in the range $(-r_n, r_d)$ for every trailing coefficient. The corresponding integer for one coefficient was randomly chosen to be fixed at r_n. We then set

$$|a_e| = \left(\frac{r_n}{r_d}\right)^{d-|e|} \binom{d}{e}$$

and defined $f = x^d +$ trailing polynomial.

In Figure 4.4, we plot the log of the average improvement of $B_{New,2}$ for 100 monic polynomials of degree 4 and given $B - Height$. We see similar plots both for other degrees and other choices of the norm ($B_{New,k}$ with $k \neq 2$). As we can see from Figure 4.4, the improvement increases as the magnitude of the roots becomes much different from 1.

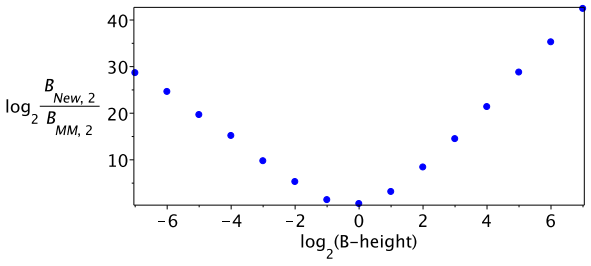

Figure 4.4: Average Improvement for given $B-$Height and Degree 4

We will also study the experimental performance of the new bound on a special class of polynomials known as Mignotte polynomials [38]. A Mignotte polynomial is defined as

$$Mig(d, h) = x^d - 2(hx - 1)^2$$

It is well known that Mignotte polynomials have very small root separation. In Figure 4.5, we plot the log of the improvement of $B_{New,2}$ when h is fixed at 10 and degree varies, and the log of the improvement of $B_{New,2}$ when the degree is fixed at 3 and h varies.

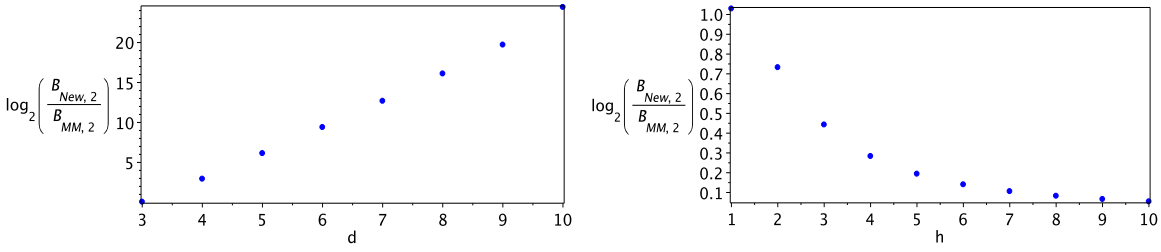

Figure 4.5: Improvement for Mignotte Polynomials

Chapter 5

Root Separation Bounds of Polynomial Systems

In this chapter we present a new improved root separation bound for polynomial systems. Unsurprisingly, known root separation bounds on polynomial systems suffer from the same issues as their univariate counterparts. Namely, they are very pessimistic and they do not scale correctly. So we face the same challenge as in the proceeding chapter: we want to find new root separation bounds such that

1. the new bounds are less pessimistic (or almost always less pessimistic) than known bounds
2. the new bounds scale correctly
3. and of course, the new bounds can be computed efficiently.

The main contribution of this chapter is to provide a new root separation bound for polynomial systems which meets the challenge. We derive the new bound using a similar strategy as in the univariate case. We will transform a known bound into a new bound which meets the challenge. The bound we will transform is the bound due to Emiris, Mourrain, and Tsigaridas [18] (discussed in Chapter 2). While the overall strategy is the same as in the univariate case, we will see that the derivation of the new multivariate bound requires completely new tools which were not required to derive the univariate bound. Experimental evidence again indicates that the improvement is usually very large, especially when the magnitude of roots are different from 1.

The structure of this chapter is as follows. In Section 5.1 we present the new univariate bound which meets the challenge. In Section 5.2 we derive the new bound. In Section 5.3 we discuss the experimental performance of the new bound.

5.1 Main Result

In this section we will precisely state the main result of the chapter. We require the following notation.

Notation 5.1.

$$\begin{aligned}
\mathbb{F}_n &= \{F \in (\mathbb{C}[x_1,\ldots,x_n])^n : \ F \text{ has finitely many (at least two) solutions,} \\
&\qquad\qquad \text{and all solutions are simple.}\} \\
F &= (f_1,\ldots,f_n) \in \mathbb{F}_n \\
\Delta(F) &= \min_{\substack{\beta_1\neq\beta_2\in\mathbb{C}^n \\ F(\beta_1)=F(\beta_2)=0}} ||\beta_1-\beta_2||_2 \\
dis(f) &= a_d^{2d-2}\prod_{i\neq j}(\alpha_i-\alpha_j) \\
E(f) &= Support(f) \\
d_i &= \deg(f_i) \\
D &= d_1\cdots d_n \\
M_i &= \prod_{j\neq i} d_j
\end{aligned}$$

Definition 5.1. A function $B : \mathbb{F}_n \to \mathbb{R}_+$ is a *root separation bound* if $B(F) \leq \Delta(F)$ for all $F \in \mathbb{F}_n$.

We begin by recalling the multivariate bound due to Emiris, Mourrain, and Tsigaridas [18]

$$B_{EMT}(F) = \frac{\sqrt{|dis(T_{f_0})|}}{\left(\prod_{i=1}^n ||f_i||^{M_i}\right)^{D-1}} P(d_1,\ldots,d_n,n)$$

where

$$\begin{aligned}
P(d_1,\ldots,d_n,n) &= \frac{\sqrt{3}}{D^{D/2+1}\cdot n^{1/2} C\cdot\left(\sqrt{D+1}(n+1)^D C^D \prod_{i=1}^n \binom{d_i+n}{d_i}^{M_i}\right)^{D-1}} \\
T_{f_0} &= \text{the resultant of } (f_0,f_1,\ldots,f_n) \text{ which eliminates } \{x_1,\ldots,x_n\} \\
f_0 &= \text{a separating element in the set} \\
&\qquad \left\{u - x_1 - ix_2 - \cdots - i^{n-1}x_n : 0 \leq i \leq (n-1)\binom{D}{2}\right\} \\
C &= \left((n-1)\binom{D}{2}\right)^{n-1}
\end{aligned}$$

We are now ready to present the main contribution of this chapter: a new multivariate root separation bound.

Definition 5.2 (New Multivariate Bound)**.** Define

$$B_{New}(F) = \frac{\sqrt{|dis(T_{f_0})|}}{H^{D-1}} P(d_1, \ldots, d_n, n)$$

where

$$H = \min_{s>0} R(s)$$
$$R(s) = \frac{\prod_{i=1}^{n} || \sum_{e \in E(f_i)} s^{d_i - |e|} |a_e| \, ||_\infty^{M_i}}{s^{\frac{D}{2} - \frac{1}{D-1}}}$$

Theorem 5.1 (New Multivariate Bound)**.** We have

1. B_{New} is a root separation bound.
2. $B_{New} \geq B_{EMT}$.
3. B_{New} scales covariantly.
4. The minimizer of $R(s)$ can be computed in $\mathcal{O}(n \cdot m + n \cdot d)$ algebraic operations and comparisons using

   $$FindMinimizer\left(F, (M_1, \ldots, M_n), \frac{D}{2} - \frac{1}{D-1}\right) \quad \text{(Algorithm 6)}$$

   where

   $$m = \#\text{ monomials of } F$$
   $$d = \sum_{i=1}^{n} d_i$$

Example 5.1. Let $F = (f_1, f_2)$, where

$$f_1 = x_1^2 + x_2^2 - 100$$
$$f_2 = x_2^2 - x_1^2 - 25$$

It is simple to verify that the root separation of F is $\sqrt{150}$ (≈ 12.2). It is also simple to verify that

$$f_0 = u - x_1 - x_2$$

is a separating element in $\mathcal{F}$ (see Chapter 2 for a more detailed discussion on separating elements). We compute

$$\begin{aligned} T_{f_0} &= 4u^2 - 800u^2 + 2500 \\ \sqrt{|dis(T_{f_0})|} &= 2.40 \times 10^8 \\ P &= \sqrt{30}/48348866242924385372681011200 \\ ||f_1||_\infty &= 100 \\ ||f_2||_\infty &= 25 \\ ||f_1||_\infty^2 ||f_2||_\infty^2 &= 6.25 \times 10^6 \end{aligned}$$

Hence

$$B_{EMT}(F) \;=\; \frac{2.40 \times 10^8}{(6.25 \times 10^6)^4} \cdot \frac{\sqrt{3}}{48348866242924385372681011200} \;\approx\; 1.11 \times 10^{-40}$$

Now we compute H. We compute

$$\begin{aligned} s^* &= FindMinimizer(F, (2,2), \frac{4}{2} - \frac{1}{4-1}) \\ &= 1.00 \times 10^{-1} \end{aligned}$$

Hence

$$\begin{aligned} H &= R(s^*) \\ &= 4.64 \times 10^1 \end{aligned}$$

Hence

$$B_{New}(F) = \frac{2.40 \times 10^8}{(4.64 \times 10^1)^4} \cdot \frac{\sqrt{3}}{48348866242924385372681011200} \approx 2.71 \times 10^{-25}$$

Note that this number is still quite pessimistic; however, the new bound is significantly larger than $B_{EMT}(F)$. To demonstrate the covariance, we plot the function $B_{New}(\, F(x_1/s, x_2/s)\,)$ in Figure 5.1. □

Remark 5.1. Note that B_{New} is only defined for the $\infty-$norm. It turns out that generalizing the result to arbitrary norms is more difficult than in the univariate case.

Remark 5.2. For $F \in \mathbb{F}_n$, T_{f_0} is a square-free integer polynomial; hence $dis(T_{f_0})$ has a lower bound of 1. Hence in practice the discriminant is almost always replaced by 1. In this case,

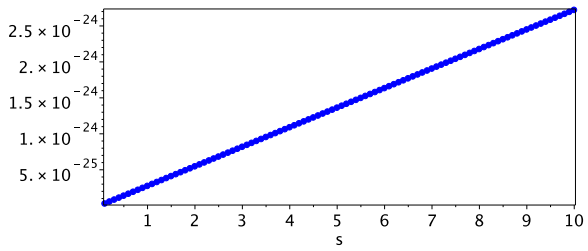

Figure 5.1: Scaling covariance of B_{New}

part (4) of Theorem 5.1 implies that B_{New} can be computed in $\mathcal{O}(n \cdot m + d \log(d))$ algebraic operations and comparisons. As with the new univariate bound, removing the discriminant sacrifices the scaling covariance.

5.2 Derivation

5.2.1 Overall framework

In this subsection, we present the framework we will use to derive the new bound. It turns out that we can use the same framework as in the previous chapter. Every proposition in this section generalizes the propositions of the previous chapter to root separation bounds on polynomial systems. The proofs are also almost identical.

As in the previous chapter, we begin by precisely defining a scaled polynomial system.

Notation 5.2.

- $F^{(s)} = (f_1^{(s)}, \ldots, f_n^{(s)})$ where $f_i^{(s)} = s^{d_i} f_i(x_1/s, \ldots, x_n/s)$.

In Propositions 5.1-5.3 we will incrementally develop the framework used to meet the challenge.

Proposition 5.1 (Scaled Bound)**.** Let $B : \mathbb{F}_n \to \mathbb{R}_+$ be a root separation bound and $s \in \mathbb{R}_+$. Let

$$B^* : F \mapsto \frac{B(F^{(s)})}{s}$$

Then

1. B^* is a root separation bound.

We will illustrate the result by a simple example, since the proof is simple.

Example 5.2. Let $F = (f_1, f_2)$, where

$$f_1 = x_1^2 + x_2^2 - 100$$
$$f_2 = x_1^2 - x_2^2 - 25$$

Then $F^{(2)} = (f_1^{(2)}, f_2^{(2)})$, where

$$\begin{aligned} f_1^{(2)} &= 2^2 \left((x_1/2)^2 + (x_2/2)^2 - 100 \right) \\ &= x_1^2 + x_2^2 - 400 \\ f_2^{(2)} &= 2^2 \left((x_1/2)^2 - (x_2/2)^2 - 25 \right) \\ &= x_1^2 - x_2^2 - 100 \end{aligned}$$

The roots of F are plotted in the left plot Figure 5.2, with the minimum root separation highlighted. In the middle of Figure 5.2 we plot the roots of $F^{(2)}$ (in orange) with the roots of F, and in the right plot we highlight the root separation of $F^{(2)}$. Note that the root separation of $F^{(2)}$ is twice the root separation of F.

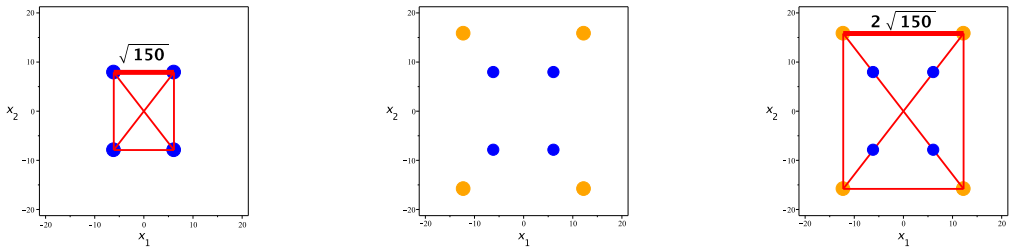

Figure 5.2: Root Separation of F and Root Separation of $F^{(2)}$

We have

$$B_{EMT}(\, F^{(2)}\,) \;=\; 4.25 \times 10^{-46}. \tag{5.1}$$

Since B_{EMT} is a root separation bound, it follows that

$$B_{EMT}(\, F^{(2)}\,) \;\leq\; \Delta(\, F^{(2)}\,) \;=\; 2\,\Delta(F)$$

Rearranging yields

$$\frac{B_{EMT}(\, F^{(2)}\,)}{2} \leq \Delta(F) \tag{5.2}$$

Combining (5.1) and (5.2) we have

$$\frac{4.25 \times 10^{-46}}{2} \;=\; 2.13 \times 10^{-46} \;\leq\; \Delta(F).$$

Note that $2.13 \times 10^{-46} \leq B_{EMT}(F)$. So 2 was not a good choice for s. As in the previous chapter, we observe that the best choice of s is the value which maximizes $B(F^{(s)})/s$. In Figure 5.3 we plot the function $B_{EMT}(\, F^{(s)}\,)/s$. The maximum value of this curve is approximately 2.7×10^{-25}, which is significantly larger than $B_{EMT}(F)$. □

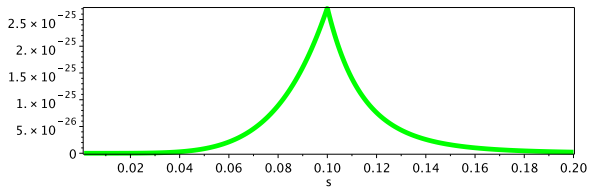

Figure 5.3: Scaled bound for B_{EMT} and F.

Proposition 5.2 (Covariant Bound)**.** Let $B : \mathbb{F}_n \to \mathbb{R}_+$ be a root separation bound and $\sigma : \mathbb{F}_n \to \mathbb{R}_+$. Let

$$B^* : F \mapsto \frac{B(F^{(\sigma(F))})}{\sigma(F)}$$

If $\forall F \in \mathbb{F}_n$ and $\forall \gamma > 0$ we have

$$\sigma(F^{(\gamma)}) = \frac{1}{\gamma}\sigma(F)$$

then

1. B^* is a root separation bound.
2. B^* scales covariantly

Proof. The first property follows from Proposition 5.1.

We will now prove the second property. Let $F \in \mathbb{F}_n$ and $\gamma > 0$. By definition

$$B^*(f^{(\gamma)}) \;=\; \frac{B\left(\left(F^{(\gamma)}\right)^{(\sigma(F^{(\gamma)}))}\right)}{\sigma(F^{(\gamma)})}$$

Since $\sigma(F^{(\gamma)}) = \frac{1}{\gamma}\sigma(F)$, we have

$$\left(F^{(\gamma)}\right)^{(\sigma(F^{(\gamma)}))} = F^{(\gamma\sigma(F^{(\gamma)})} = F^{(\gamma\cdot\frac{1}{\gamma}\cdot\sigma(F))} = F^{(\sigma(F))} \tag{5.3}$$

Hence

$$\begin{aligned} B^*(F^{(\gamma)}) &= \frac{B\left(\left(F^{(\gamma)}\right)^{\sigma(F^{(\gamma)})}\right)}{\sigma(F^{(\gamma)})} = \frac{B(F^{(\sigma(F))})}{\sigma(F^{(\gamma)})} && \text{from (5.3)} \\ &= \frac{B(F^{(\sigma(F))})}{\frac{1}{\gamma}\sigma(F)} = \gamma\frac{B(F^{(\sigma(F))})}{\sigma(F)} = \gamma B^*(F) \end{aligned}$$

We have proved that B^* scales covariantly. □

Proposition 5.3 (Optimal Bound)**.** Let $B : \mathbb{F}_n \to \mathbb{R}_+$ be a root separation bound. Let

$$B^* : F \mapsto \max_s \frac{B(F^{(s)})}{s}$$

Then

1. B^* is a root separation bound.
2. B^* scales covariantly
3. $B^*(F) \geq B(F)$

Proof. The first property follows from Proposition 5.1.

To prove the second property, we will show that σ has the scaling property described in Proposition 5.2. Let $F \in \mathbb{F}_n$ and $\gamma > 0$. We have

$$\begin{aligned} \sigma(F^{(\gamma)}) &= \arg\max_{s>0} \frac{B\left(\left(F^{(\gamma)}\right)^{(s)}\right)}{s} \\ &= \arg\max_{s>0} \frac{B\left(F^{(\gamma s)}\right)}{s} \\ &= \arg\max_{s>0} \frac{1}{\gamma}\frac{B\left(F^{(\gamma s)}\right)}{s} && \text{since } \gamma > 0 \\ &= \arg\max_{s>0} \frac{B\left(F^{(\gamma s)}\right)}{s\gamma} \end{aligned}$$

$$= \frac{1}{\gamma} \arg\max_{s>0} \frac{B\left(\, F^{(s)} \,\right)}{s}$$

$$= \frac{1}{\gamma}\sigma(f)$$

Hence by Proposition 5.2, B^* scales covariantly.

We will now prove the third property. We have

$$B^*(F) = \max_{s>0} \frac{B(\, F^{(s)}\,)}{s} \geq \frac{B(\, F^{(1)}\,)}{1} = \frac{B(F)}{1} = B(F)$$

We have proved the Proposition. □

Let us summarize the framework built up in this section. We have seen that

$$\max_{s>0} \frac{B(F^{(s)})}{s}$$

meets the challenge *if the maximum can be computed efficiently*. In the previous chapter, we were not able to compute the maximum value for $B_{MM,k}$ efficiently; instead, we had to approximate the maximum. In this chapter we will see that we can compute the maximum for B_{EMT} efficiently. As a consequence, Properties 2 and 3 (scaling covariance and guaranteed improvement) will follow immediately, with no extra derivation required.

5.2.2 Derivation of New Multivariate Bound

In this subsection, we derive the new multivariate bound. For the remainder of this subsection, let $F \in \mathbb{F}_n$ be fixed, and f_0 a fixed separating element of F. Similar to the previous chapter, we will begin by deriving a simplified expression for

$$s^* = \arg\max_{s>0} \frac{B_{EMT}(\, F^{(s)}\,)}{s}.$$

We first need to understand the affect that root scaling has on the discriminant of T_{f_0}. We make of use the following result from the proof of Proposition 5.8 of [13].

Lemma 5.1. Let F be zero-dimensional, have no solutions at infinity, and have no singular solutions. Let

$$f_0 = u + r_1x_1 + \cdots + r_nx_n$$

and T_{f_0} be the resultant of (F, f_0) which eliminates $(x_1, \ldots, x_n)$. Then

$$T_{f_0} = C \prod_{\gamma \in V(F)} f_0(\gamma)$$

where

$$\begin{aligned} C &= Res(\widehat{F}) \\ \widehat{F} &= (\widehat{f_1}, \ldots, \widehat{f_n}) \\ \widehat{f_i} &= \sum_{\substack{e \in E(f_i) \\ |e| = d_i}} a_e \mathbf{x}^e \end{aligned}$$

Lemma 5.2. Let $s > 0$. Let $T_{f_0}^{(s)}$ be the resultant of $F^{(s)}$ and f_0. Then

$$dis(T_{f_0}^{(s)}) = s^{D(D-1)} dis(T_{f_0})$$

Proof. To prove the claim, we will first show that the leading coefficients of T_{f_0} and $T_{f_0}^{(s)}$ are the same. Then we will use the definition of the discriminant to complete the proof.

Let C be the leading coefficient of T_{f_0} and $C_{f_0}^{(s)}$ the leading coefficient of $T^{(s)}$. From Lemma 5.1, we have

$$C = Res(\widehat{F}) \text{ and } C^{(s)} = Res(\widehat{F}^{(s)}) \tag{5.4}$$

Note that

$$\begin{aligned} \widehat{f_i^{(s)}} &= s^{d_i} f_i(\widehat{x_1/s}, \ldots, x_n/s) \\ &= s^{d_i} \sum_{|e|=d_i} a_e \left(\mathbf{x}^{(s)}\right)^e \\ &= s^{d_i} \sum_{|e|=d_i} a_e \left(\frac{x_1}{s}\right)^{e_1} \cdots \left(\frac{x_n}{s}\right)^{e_n} \\ &= s^{d_i} \sum_{|e|=d_i} \left(\frac{1}{s}\right)^{e_1+\cdots+e_n} a_e x_1^{e_1} \cdots x_n^{e_n} \\ &= s^{d_i} \sum_{|e|=d_i} \left(\frac{1}{s}\right)^{e_1+\cdots+e_n} a_e \mathbf{x}^e \\ &= s^{d_i} \sum_{|e|=d_i} \left(\frac{1}{s}\right)^{d_i} a_e \mathbf{x}^e \\ &= s^{d_i} \left(\frac{1}{s}\right)^{d_i} \sum_{|e|=d_i} a_e \mathbf{x}^e \end{aligned}$$

$$= \sum_{|e|=d_i} a_e \mathbf{x}^e$$
$$= \widehat{f_i}$$

Hence

$$\widehat{F} = \widehat{F^{(s)}} \tag{5.5}$$

Combining (5.4) and (5.5), we have

$$C = C^{(s)} \tag{5.6}$$

Note that the roots T_{f_0} are

$$\{r_1\gamma_{i,1} + \cdots + r_n\gamma_{i,n}\}_{i=1}^{D}$$

and the roots of $T_{f_0}^{(s)}$ are

$$\{s \cdot (r_1\gamma_{i,1} + \cdots + r_n\gamma_{i,n})\}_{i=1}^{D}$$

We will now expand the discriminant of $T_{f_0}^{(s)}$. We have

$$\begin{aligned}
dis(T_{f_0}^{(s)}) &= \left(C^{(s)}\right)^{D(D-1)} \prod_{i\neq j} (s \cdot (r_1\gamma_{i,1} + \cdots + r_n\gamma_{i,n}) - s \cdot (r_1\gamma_{j,1} + \cdots + r_n\gamma_{j,n})) \\
&= C^{D(D-1)} \prod_{i\neq j} (s \cdot (r_1\gamma_{i,1} + \cdots + r_n\gamma_{i,n}) - s \cdot (r_1\gamma_{j,1} + \cdots + r_n\gamma_{j,n})) \qquad \text{from (5.6)} \\
&= s^{D(D-1)} C^{D(D-1)} \prod_{i\neq j} ((r_1\gamma_{i,1} + \cdots + r_n\gamma_{i,n}) - (r_1\gamma_{j,1} + \cdots + r_n\gamma_{j,n})) \\
&= s^{D(D-1)} dis(T_{f_0})
\end{aligned}$$

□

Lemma 5.3. Let $s > 0$. Then

$$\frac{B_{EMT}(F^{(s)})}{s} = \frac{\sqrt{|dis(T_{f_0})|}}{R(s)^{D-1}} P(d_1, \ldots, d_n, n)$$

where

$$R(s) = \frac{\prod_{i=1}^{n} ||f_i^{(s)}||_\infty^{M_i}}{s^{\frac{D}{2} - \frac{1}{D-1}}}$$

Proof. We have

$$\frac{B_{EMT}(F^{(s)})}{s} = \frac{1}{s} \frac{\sqrt{|dis(T_{f_0}^{(s)})|}}{\prod_{i=1}^{n} ||f_i^{(s)}||_\infty^{M_i(D-1)}} P(d_1, \ldots, d_n, n)$$

$$= \frac{1}{s} \frac{s^{\frac{D(D-1)}{2}} \sqrt{|dis(T_{f_0})|}}{\left(\prod_{i=1}^{n} ||f_i^{(s)}||_\infty^{M_i}\right)^{D-1}} P(d_1, \ldots, d_n, n) \qquad \text{from Lemma 5.2}$$

$$= \frac{\sqrt{|dis(T_{f_0})|}}{\left(\frac{\prod_{i=1}^{n} ||f_i^{(s)}||_\infty^{M_i}}{s^{\frac{D}{2} - \frac{1}{D-1}}}\right)^{D-1}} P(d_1, \ldots, d_n, n)$$

$$= \frac{\sqrt{|dis(T_{f_0})|}}{R(s)^{D-1}} P(d_1, \ldots, d_n, n)$$

□

Lemma 5.4. We have

$$s^* = \arg\min_{s>0} R(s)$$

Proof. To prove the claim, we will again make use of the identities in Lemma 4.1 . We have

$$\arg\max_{s>0} \frac{B_{EMT}(F^{(s)})}{s} = \arg\max_{s>0} \frac{\sqrt{|dis(T)|}}{R(s)^{D-1}} P(d_1, \ldots, d_n, n) \qquad \text{from Lemma 5.3}$$

$$= \arg\max_{s>0} \frac{1}{R(s)^{D-1}} \qquad \text{(Identity 1)}$$

$$= \arg\max_{s>0} \frac{1}{R(s)} \qquad \text{(Identity 2)}$$

$$= \arg\min_{s>0} R(s) \qquad \text{(Identity 3)}$$

□

We will now consider the computation of $\arg\min_{s>0} R(s)$. For the sake of generality, we will study all functions of the form

$$R(s) = \frac{\prod_{i=1}^{n} ||f_i^{(s)}||_\infty^{U_i}}{s^V}$$

where $U_1, \ldots, U_n, V \in \mathbb{R}_{>0}$. Let $s^* = \arg\min_{s>0} R(s)$. We will show that s^* can be computed in $\mathcal{O}\left(n \cdot m + n \cdot d \right)$ algebraic operations and comparisons. Our overall strategy will be to transform the problem into a new problem which is stated in terms of *linear* functions. More precisely, we will show that $\log(R(s))$ can be viewed as the *upper envelope* of a set of linear functions. We will make use of a technique for efficiently computed upper envelopes known as the *Convex Hull Trick* to compute s^* efficiently.

Lemma 5.5. Let $t = \log(s)$. We have

$$\log(R(s)) = \sum_{i=1}^{n} U_i \cdot \max_{e \in E(f_i)} \left((d_i - |e|) \cdot t + \log(|a_e|) \right) - V \cdot t$$

Proof. We have

$$\begin{aligned} \log(R(s)) &= \log \left(\frac{\prod_{i=1}^{n} ||f_i^{(s)}||^{U_i}}{s^V} \right) \\ &= \sum_{i=1}^{n} U_i \cdot \log(||f_i^{(s)}||) - V \cdot \log(s) \end{aligned} \tag{5.7}$$

Note that

$$\begin{aligned} \log(||f_i^{(s)}||) &= \log \left(\max_{e \in E(f_i)} s^{d_i - |e|} |a_e| \right) \\ &= \max_{e \in E(f_i)} \left(\log \left(s^{d_i - |e|} |a_e| \right) \right) \\ &= \max_{e \in E(f_i)} \left((d_i - |e|) \cdot \log(s) + \log(|a_e|) \right) \\ &= \max_{e \in E(f_i)} \left((d_i - |e|) \cdot t + \log(|a_e|) \right) \end{aligned} \tag{5.8}$$

Combining (5.7) and (5.8), we have

$$\log(R(s)) = \sum_{i=1}^{n} U_i \cdot \max_{e \in E(f_i)} \left((d_i - |e|) \cdot t + \log(|a_e|) \right) - V \cdot t$$

□

Since the sum of upper envelopes is an upper envelope, $\log(R(s))$ is an upper envelope. The upper envelope of a set of linear functions $l_i(t) = \beta_i \cdot t + \xi_i$ on $t > 0$ is represented by an ordered sequence $(l_{i_1}, 0), (l_{i_2}, t_{i_1,i_2}), \ldots, (l_{i_r}, t_{i_{r-1},i_r})$ such that

$$\max_i \ l_i(t) = \begin{cases} l_{i_1}(t) & -\infty \leq t \leq t_{i_1,i_2} \\ l_{i_2}(t) & t_{i_1,i_2} \leq t \leq t_{i_2,i_3} \\ \vdots & \\ l_{i_r}(t) & t_{i_{r-1},i_r} \leq t \leq \infty \end{cases}$$

Given such a representation, finding the t which minimizes the upper envelope is trivial: we simply find the corner point t where the slopes of the lines in the upper envelope switch from

negative to positive. In fact, this representation contains more information than is necessary to find the minimizer. We need only store the slopes of functions which lie on the upper envelope, as well as the corner points.

Hence we have the following initial strategy. For $i = 1, \ldots, n$, we compute the upper envelope representation of

$$\max_{e \in E(f_i)} \left((d_i - |e|) \cdot t + \log(|a_e|) \right) \tag{5.9}$$

The most efficient algorithm for computing upper envelope representations of linear functions is known as the Convex Hull Trick. It is not clear who deserves credit for this trick; it appears to be folklore, not published in the literature. See [1] for a concise summary. We can combine the upper envelope representations to find the representation of

$$\log(R(s)) = \sum_{i=1}^{n} U_i \cdot \max_{e \in E(f_i)} \left((d_i - |e|) \cdot t + \log(|a_e|) \right) - V \cdot t$$

We then read off the minimizer t^* of $\log(R(s))$ and return

$$s^* = e^{t^*}$$

We will now discuss improvements to the above strategy. Note that in the above strategy we must take logarithms. Recall that the current goal is to present an algorithm which produces the minimizer in

$$\mathcal{O}(n \cdot m + n \cdot d)$$

algebraic operations and comparisons. It turns out that is a relatively trivial matter to modify the Convex Hull Trick algorithm to avoid logarithm computations for the current application. In the Convex Hull Trick algorithm, we compare corner points t_{i_1,i_2} and t_{i_3,i_4}. In our case, the corner points for the upper envelope of (5.9) are the points where

$$(d_i - |e_1|) \cdot t + \log(|a_{e_1}|) = (d_i - |e_2|) \cdot t + \log(|a_{e_2}|).$$

The above equality holds if and only if

$$t = \frac{\log(|a_{e_1}|) - \log(|a_{e_2}|)}{|e_1| - |e_2|} = \log\left(\left(\frac{|a_{e_1}|}{|a_{e_2}|} \right)^{\frac{1}{|e_1| - |e_2|}} \right).$$

Clearly,

$$\log\left(\left(\frac{|a_{e_1}|}{|a_{e_2}|} \right)^{\frac{1}{|e_1| - |e_2|}} \right) \leq \log\left(\left(\frac{|a_{e_3}|}{|a_{e_4}|} \right)^{\frac{1}{|e_3| - |e_4|}} \right) \iff \left(\frac{|a_{e_1}|}{|a_{e_2}|} \right)^{\frac{1}{|e_1| - |e_2|}} \leq \left(\frac{|a_{e_3}|}{|a_{e_4}|} \right)^{\frac{1}{|e_3| - |e_4|}}.$$

We can use this equivalence to perform all of the necessary comparisons in the Convex Hull Trick algorithm without computing any logarithms.

It is also possible to speed up the computation of the upper envelope representations by making use of the following Lemma.

Lemma 5.6. Let $s > 0$. Then

$$||f^{(s)}||_\infty = \max_{0 \le k \le \deg(f)} s^{d-k} \cdot b_k$$

where

$$d = \deg(f)$$
$$b_k = \max_{\substack{e \in E(f) \\ |e|=k}} |a_e|$$

Proof. Note that

$$f^{(s)} = s^d f(x_1/s, \ldots, x_n/s) = s^d \cdot \sum_{e \in E(f)} a_e \left(\frac{x_1}{s}\right)^{e_1} \left(\frac{x_2}{s}\right)^{e_2} \cdots \left(\frac{x_1}{s}\right)^{e_n} = \sum_{e \in E(f)} s^{d-|e|} a_e \cdot x^e$$

Hence

$$\begin{aligned}
||f^{(s)}||_\infty &= \max_{e \in E(f)} s^{d-|e|} |a_e| \\
&= \max_{0 \le k \le d} \left\{ \max_{\substack{e \in E(f) \\ |e|=k}} s^{d-|e|} |a_e| \right\} \\
&= \max_{0 \le k \le d} \left\{ \max_{\substack{e \in E(f) \\ |e|=k}} s^{d-k} |a_e| \right\} \\
&= \max_{0 \le k \le d} s^{d-k} \left\{ \max_{\substack{e \in E(f) \\ |e|=k}} |a_e| \right\} \\
&= \max_{0 \le k \le d} s^{d-k} \cdot b_k
\end{aligned}$$

□

We are now ready to present *FindMinimizer* (Algorithm 6). For each f_i, we first find the coefficient of largest magnitude for each total degree (Lemma 5.6). We then use the sub-algorithm *UpperEnvelopeSlopes* (Algorithm 5) to compute the slopes of the lines which lie on

the upper envelope of $\log(||f_i^{(s)}||_\infty)$, as well as the points s_{e_i,e_j} such that $t_{e_i,e_j} = \log(s_{e_i,e_j})$ is a corner point of the upper envelope. *UpperEnvelopeSlopes* is a straightforward modification of the Convex Hull Trick algorithm. Once the upper envelope slopes are computed for each $\log(||f_i^{(s)}||_\infty)$, we search for the smallest s such that the slope of $\log(R)$ is positive for $t > \log(s)$.

We are now ready to discuss the complexity of $FindMinimizer$.

Lemma 5.7. Let $U_1, \ldots, U_n, V \in \mathbb{R}_{>0}$ and

$$R(s) = \frac{\prod_{i=1}^n ||f_i^{(s)}||_\infty^{U_i}}{s^V}$$

Then

$$\arg\min_{s>0} R(s)$$

can be computed in $\mathcal{O}(\ n \cdot m + n \cdot d)$ algebraic operations and comparisons, where

$$m = \#\text{ monomials of } F$$
$$d = \sum_{i=1}^n d_i$$

Proof. We consider the total time spent on each line of $FindMinimizer$.

In Line 3, we compute

$$L_i \leftarrow [((d_i - k),\ \ 0), \quad k = 0, \ldots, d_i]$$

which requires a total of $\mathcal{O}(\sum_{i=0}^n d_i)$ algebraic operations.

In Lines 5 and and 6 we check and potentially update the entry $L_i[|e|][2]$. This is done for every $e \in E(f_i)$. Since the computation of $|e|$ requires $\mathcal{O}(n)$ algebraic operations, the number of algebraic operations in lines $5-6$ is $\mathcal{O}(n \cdot \sum_{i=1}^n \#E(f_i)) = \mathcal{O}(n \cdot m)$.

In Line 7 we compute

$$Z_i \leftarrow UpperEnvelopeSlopes(L_i)$$

It is straightforward to see that *UpperEnvelopeSlopes* requires $\mathcal{O}(r)$ algebraic operations and comparisons when r linear functions are input. Since L_i has $\mathcal{O}(d_i)$ elements, line 7 requires $\mathcal{O}(d_i)$ algebraic operations and comparisons. Hence the total amount of work performed in Line 9 is $\mathcal{O}(\sum_{i=1}^n d_i)$.

In Line 8 we compute

$$M \leftarrow \text{the list of triples } (\beta, i, s), \text{ sorted in ascending order with respect to } s$$

Algorithm 5: *UpperEnvelopeSlopes*

Input : $L = [l_1, \ldots, l_r]$ where
$l_i(t) = \beta_i \cdot t + \log(\xi_i)$
$\xi_i > 0$ for all i
$0 \leq \beta_1 < \beta_2 < \ldots \beta_r$
$l_i(t)$ is represented by (β_i, ξ_i)

Output: M: an ordered list $[(\beta_{i_1}, 0), (\beta_{i_2}, s_{i_1,i_2}), \ldots, (\beta_{i_r}, s_{i_{r-1},i_r})]$ such that

$$\max_i \; l_i(t) = \begin{cases} \beta_{i_1} \cdot t + \log(\xi_{i_1}) & -\infty \leq t \leq t_{i_1,i_2} \\ \beta_{i_2} \cdot t + \log(\xi_{i_2}) & t_{i_1,i_2} \leq t \leq t_{i_2,i_3} \\ ; \;\; \vdots & \\ \beta_{i_r} \cdot t + \log(\xi_{i_r}) & t_{i_{r-1},i_r} \leq t \leq \infty \end{cases}$$

where $t_{i_j,i_k} = \log(s_{i_j,i_k})$.

begin
  // L will store the indices of the linear functions which lie on the upper envelope in the order which they appear. We construct L using a slight modification of the Convex Hull Trick algorithm.
  $L \leftarrow [1]$;
  for i *from* 2 *to* r **do**
    Append i to L;
    while $size(L) > 2$ *and* $\left(\frac{\xi_{L[size(L)-1]}}{\xi_{L[size(L)]}}\right)^{\frac{1}{\beta_{L[size(L)]} - \beta_{L[size(L)-1]}}} < \left(\frac{\xi_{L[size(L)-2]}}{\xi_{L[size(L)-1]}}\right)^{\frac{1}{\beta_{L[size(L)-1]} - \beta_{L[size(L)-2]}}}$ **do**
      Remove $L[size(L) - 1]$ from L;
  $M \leftarrow [(\beta_{L[1]}, 0)]$;
  for i *from* 2 *to* $size(L)$ **do**
    Append $\left(\beta_{L[i]}, \left(\frac{\xi_{L[i-1]}}{\xi_{L[i]}}\right)^{\frac{1}{\beta_{L[i]} - \beta_{L[i-1]}}}\right)$ to M;
end

Algorithm 6: *FindMinimizer*

Input : F, U, V

Output: $s^* = \arg\min_{s>0} \frac{\prod_{i=1}^{n} ||f_i^{(s)}||_\infty^{U_i}}{s^V}$

begin
  for i *from* 1 *to* n *do* **do**
    $L_i \leftarrow [((d_i - k),\ 0), \quad k = 0, \ldots, d_i]$ `// Lines are represented by` $(\texttt{slope}, e^{intercept})$;
    for $e \in E(f_i)$ **do**
      if $L_i[|e|][2] < |a_e|$ **then**
        $L_i[|e|][2] = |a_e|$ `// Find the largest magnitude coefficient for each degree (Lemma 5.6);`
    $Z_i \leftarrow UpperEnvelopeSlopes(L_i)$;
  $M \leftarrow$ the list of triples (β, i, s), sorted in ascending order with respect to s, where (β, s) is an element of Z_i;
  `// Search for the first` s `where` $\log(R)$ `has positive slope after` $\log(s)$:
  $C \leftarrow [0, \ldots, 0]$`//` $C[i]$ `stores the slope of` $\log(||f_i^{(s)}||_\infty)$;
  for m *in* M **do**
    $C[m[2]] = m[1]$`// Update the slope for` $\log(||f_i^{(s)}||_\infty)$;
    $\alpha \leftarrow U_1 \cdot C[1] + \cdots + U_n \cdot C[n] - V$`// Calculate the slope of` $\log(R)$ `for` t `immediately after` $\log(s) = \log(m[3])$;
    if $\alpha > 0$ **then**
      return $m[3]$;
end

where (β, s) is an element of Z_i

Note that every list Z_i is already sorted in ascending order with respect to s, and Z_i has $\mathcal{O}(d_i)$ elements. Hence constructing M requires $\mathcal{O}(n \cdot \sum_{i=1}^{n} d_i)$ algebraic operations and comparisons.

Line 9 can clearly be computed in a constant number of algebraic operations.

In the remainder of the algorithm, we potentially loop over all $\mathcal{O}(\sum_{i=1}^{n} d_i)$ elements of M. Lines 11 and 13 both require a constant number of algebraic operations and comparisons. Line 12 requires $\mathcal{O}(n)$ algebraic operations. Hence the total number of algebraic operations and comparisons performed in lines $10 - 14$ is $\mathcal{O}(n \cdot \sum_{i=1}^{n} d_i)$

Combining all of the above, the total number of algebraic operations and comparisons required to compute $FindMinimizer(F, U, V)$ is

$$\mathcal{O}\left(n \cdot \sum_{i=1}^{n} \#E(f_i) + n \cdot \sum_{i=1}^{n} d_i\right) = \mathcal{O}\left(n \cdot m + n \cdot d\right)$$

□

We are now ready to prove Theorem 5.1.

Proof of Theorem 5.1. Note that

$$\begin{aligned} B_{New}(F) &= \frac{\sqrt{|dis(T_{f_0})|}}{R(s^*)^{D-1}} P(d_1, \ldots, d_n, n) \\ &= \frac{\sqrt{|dis(T_{f_0})|}}{\left(\arg\min_{s>0} R(s)\right)^{D-1}} P(d_1, \ldots, d_n, n) \\ &= \max_{s>0} \frac{B_{EMT}(F^{(s)})}{s} \qquad \text{from Lemma 5.3} \end{aligned}$$

Hence parts $1, 2$ and 3 of the Theorem follow immediately from Proposition 5.3. The fourth part follows from Lemmas 5.3 and 5.7. □

5.3 Performance

In this Section, we discuss the experimental performance of the new bound. We have observed that the improvement is usually very large for the new bound, especially when the magnitude of roots are different from 1. To generate data points, we generated 100 random square Pham polynomial systems with fixed degree and height (defined below) and calculated the average

value of the improvement:

$$\frac{B_{New}(F)}{B_{EMT}(F)} = \left(\frac{\prod_{i=1}^{n} ||f_i||^{M_i}}{H}\right)^{D-1}$$

Note that the improvement is independent of the discriminant for the new bound. This observation allowed us to avoid many expensive computations when performing experiments (in particular, no resultants need be computed). We extended the binomial height used in the previous chapter Pham polynomials of degree d with the definition

$$||f||_B = \max_{e \in Support(\text{trailing polynomial of } f)} \frac{|a_e|^{\frac{1}{d-|e|}}}{\binom{d}{e}}$$

It is well known this height is linearly related to the size of the roots. To generate a polynomial system with the height r_n/r_d, we uniformly generated an integer c in the range $(-r_n, r_d)$ for every trailing coefficient. The corresponding integer for one coefficient was randomly chosen to be fixed at r_n. We then set

$$|a_e| = \left(\frac{r_n}{r_d}\right)^{d-|e|} \binom{d}{e}$$

and defined $f_i = x_i^d + \text{trailing polynomial}$.

In Figure 5.4, we plot the log of the average improvement of B_{New} for 100 Pham systems with $n = 3$ and the degree of every polynomial 3. We see similar plots both for other degrees and other choices of n. As we can see from Figure 5.4, the improvement increases as the magnitude of the roots becomes much different from 1.

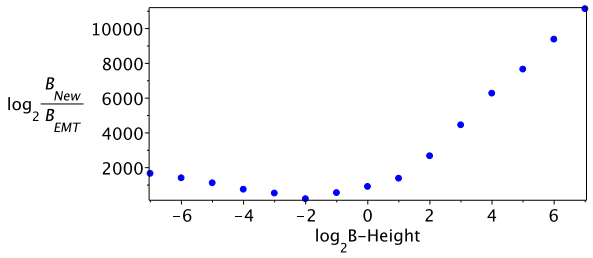

Figure 5.4: $B-$Height and Multivariate Improvement

REFERENCES

[1] Convex hull trick. `http://wcipeg.com/wiki/Convex_hull_trick`.

[2] A. Akritas, A. Strzebonksi, and P. Vigklas. Implementations of a New Theorem for Computing Bounds for Positive Roots of Polynomials. *Computing 78*, 2006.

[3] A. Akritas and P. Vigklas. A Comparison of Various Methods for Computing Bounds for Positive Roots of Polynomials. *Journal of Universal Computer Science*, 13, 2007.

[4] P. Batra. A property of the nearly optimal root-bound. *Journal of Computational and Applied Mathematics*, 167, 2004.

[5] P. Batra. A Lower Bound for the Separation of Polynomials. 2008.

[6] P. Batra and V. Sharma. Bounds on Absolute Positiveness of Multivariate Polynomials. *Journal of Symbolic Computation*, 2010.

[7] Y. Bugeaud and M. Mignotte. On the Distance Between Roots of Integer Polynomials. *Proc. Edinburgh Math. Soc. 47 (3)*, pages 553–556, 2004.

[8] C. Burnikel, S. Funke, K. Melhorn, S. Schirra, and S. Schmitt. A Separation Bound for Real Algebraic Expressions. *Lecture Notes in Computer Science*, pages 254–265, 2001.

[9] M. Burr, S.W. CHoi, B. Galehouse, and C.K. Yap. Complete subdivision algorithms. In *Proc. of Annual ACM Symp. on Symbolic and Algebraic Computation (ISAAC)*, 2008.

[10] A. Cauchy. Sur la Résolution des Équation Numériques et Sur la Théorie de l'Élimination. *Œvres Complètes*, 9, 1829.

[11] G. Collins. Polynomial Minimum Root Separation. *Journal of Symbolic Computation*, 2011.

[12] G. Collins and E. Horowitz. The Minimum Root Separation of a Polynomial. *Mathematics of Computation, Volume 28, Number 126*, 1974.

[13] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer, 2nd edition, 2005.

[14] J. H. Davenport. Cylindrical algebraic decomposition. Technical report, School of Mathematical Sciences, Univ. Bath, 1988.

[15] J.-P. Dedieu. Estimations for the Separation Number of a Polynomial System. *Journal of Symbolic Computation*, 1997.

[16] M. Dehmer and A. Mowshowitz. Bounds on the moduli of polynomial zeros. *Applied Mathematics and Computation*, 2011.

[17] A. Eigenwillig, V. Sharma, and C. K. Yap. Almost tight recursion tree bounds for the descartes method. In *Proc. Annual ACM Symp. on Symbolic and Algebraic Computation (ISAAC)*, 2006.

[18] I. Emiris, B. Mourrain, and E. Tsigaridas. The DMM Bound: Multivariate (Aggregate) Separation Bounds. *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 243–250, 2010.

[19] I. Emiris and E. Tsigaridas. Comparing Real Algebraic Numbers of Small Degree. *Lecture Notes in Computer Science Volume 3221*, 2004.

[20] M. Fujiwara. Uber die Wurzeln der algebraischen Gleichungen. *Tohoku Math. Journal*, 1915.

[21] L. Gonzalez-Vega and G. Trujillo. Multivariate Sturm-Habicht sequences: Real root counting on n-rectangles and triangles. *Real Algebraic and Analytic Geometry*, 1997.

[22] H. Hong. Bounds for Absolute Positiveness of Multivariate Polynomials. *Journal of Symbolic Computation*, 1998.

[23] V.K. Jain. On the zeros of polynomials ii. *Journal of Mathematical and Physical Sciences*, 1986.

[24] J.R. Johnson. Algorithms for Polynomial Real Root Isolation. *PhD Thesis, Ohio State University*, 1991.

[25] A. Joyal, G. Labelle, and Q.I. Rahman. On the location of polynomials. *Canadian Mathematical Bulletin*, (10), 1967.

[26] B. Kalantari. An infinite family of bounds on zeros of analytic functions and relationship to Smale's bound. *Mathematics of Computation*, 2005.

[27] J. B. Kioustelidis. Bounds for Positive Roots of Polynomials. *Journal of Computational and Applied Mathematics 16*, 1986.

[28] J. Kojima. On a theorem of Hadamard and its applications. *Tohoku Mathematical Journal*, 1914.

[29] M. Kuniyeda. Notes on the Roots of Algebraic Equations. *Tohoku Math. Jounral*, 1916.

[30] J. L. Lagrange. Traité de la Résolution des Équations Numériques de Tous les Degrés. *Œvres de Lagrange*, 8, 1879. Reprinted from the second edition of 1808.

[31] C. Li, S. Pion, and C.Yap. Recent Progress in Exact Geometric Computation. *Journal of Logic and Algebraic Programming*, 2004.

[32] C. Li, S. Pion, and C.K. Yap. Recent progress in exact geometric computation. *The Journal of Logic and Algebraic Programming*, 2005.

[33] K. Mahler. An Inequality for the Discriminant of a Polynomial. *The Michigan Mathematical Journal*, 1964.

[34] A. Mantzaflaris, B. Mourrain, and E. Tsigaridas. Continued fraction expansion of real roots of polynomial sytems. In *Proc. Symbolic-Numeric Computation*, 2009.

[35] M. Marden. The Geometry of Zeros of a Polynomial in a Complex Variable. *Mathematics Surveys*, 3, 1949.

[36] K. Melhorn and S. Ray. Faster Algorithms for Computing Hong's Bound on Absolute Positivity. *Journal of Symbolic Computation*, 2010.

[37] M. Mignotte. An Inequality About Factors of Polynomials. *Mathematics of Computation*, 28(128), 1974.

[38] M. Mignotte. Some inequalities about univariate polynomials. *Proceedings 1981 ACM Symposium on Symbolic and Algebraic Computation, SYMSAC 1981*, 1981.

[39] M. Mignotte. *Mathematics for computer algebra.* Spring-Verlag, 1991.

[40] M. Mignotte. On the Distance Between the Roots of a Polynomial. *Applicable Algebra in Engineering, Communication, and Computing*, 1995.

[41] M. Mignotte and D. Stefanescu. *Polynomials: an Algorithmic Approach.* Springer, 1999.

[42] C. Muresan. The Polynomial Roots Repartition and Minimum Roots Separation. *WSEAS Transactions on Mathematics*, 2008.

[43] S. Rump. Polynomial Minimum Root Separation. *Mathematics of Computation, Volume 33, Number 145*, 1979.

[44] T. Sasaki and F. Kako. An algebraic method for separating close-root clusters and the minimum root separation. *Proceedings of SNC2005*, 2005.

[45] A. Schonhage. Polynomial root separation examples. *Journal of Symbolic Computation*, 2006.

[46] C. Schultz and R. Moller. Quantifier Elimination over Real Closed Fields in the Context of Applied Description Logics. *Univ., Bibl. des Fachbereichs Informatik.*, 2005.

[47] V. Sharma. Complexity of Real Root Isolation Using Continued Fractions. *Theoretical Computer Science*, 409(2), 2008.

[48] M. Sombra. The Height of the Mixed Sparse Resultant. *American Journal of Mathematics*, 2004.

[49] D. Stefanescu. New Bounds for Positive Roots of Polynomials. *Journal of Universal Computer Science*, 11(12), 2005.

[50] D. Stefanescu. Bounds for Real Roots and Applications to Orthogonal Polynomials. *Proceedings of the 10th International Workshop on Computer Algebra in Scientific Computing*, 2007.

[51] A. Strzebonksi and E. Tsigaridas. Univariate Real Root Isolation in an Extension Field and Applications. *Arxiv*, 2011.

[52] E. Tsigaridas and I. Emiris. On the Complexity of Real Root Isolation Using Continued Fractions. *Theor. Comput. Sci., 392*, pages 158–173, 2008.

[53] E. Tsigaridas and I. Z. Emiris. Univariate polynomial real root isolation: Continued fractions revisited . *Proceedings of the 14th European Symp. of Algorithms (ESA)*, 2006.

[54] A. van der Sluis. Upper Bounds for Roots of Polynomials. *Numerische Mathematik 15*, 1970.

[55] J. C. Yakoubsohn. Numerical analysis of a bisection-exclusion method to find zeros of univariate analytic functions. *Journal of Complexity*, 2005.